EXHIBIT A

SHERIFF'S ENTRY OF SERVICE

Civil Action No. 23108528

Superior Court ☒ Magistrate Court □
State Court □ Probate Court □
Juvenile Court □

Date Filed OCTOBER 31, 2023

Georgia, COBB COUNTY

ASHLEY GLENN, ET AL.

Plaintiff

VS.

META PLATFORMS, INC.

Defendant

Garnishee

Attorney's Address

WILLIAM GREGORY DOBSON
830 MULBERRY ST. SUITE 201
MACON, GA 31201

Name and Address of Party to Served

META PLATFORMS, INC. C/O CORPORATION SERVICE COMPANY 2 SUN CT. STE
400 PEACHTREE CORNERS, GA 30092

SHERIFF'S ENTRY OF SERVICE

□ **PERSONAL**
I have this day served the defendant ______ personally with a copy of the within action and summons.

□ **NOTORIOUS**
I have this day served the defendant ______ by leaving a copy of the action and summons at his most notorious place abode in this County.

□ Delivered same into hands of ______ described as follows: age, about ______ years; weight ______ pounds; height ______ feet and ______ inches, domiciled at the residence of defendant.

☑ **CORPORATION**
Served the defendant Meta Platforms [illegible] a corporation by leaving a copy of the within action and summons with Alisha Smith
In charge of the office and place of doing business of said Corporation in this County.

□ **TACK & MAIL**
I have this day served the above styled affidavit and summons on the defendant(s) by posting a copy of the same to the door of the premises designated in said affidavit and on the same day of such posting by depositing a true copy of same in the United States Mail, First Class in an envelope properly addressed to the defendant(s) at the address shown in said summons, with adequate postage affixed thereon containing notice to the defendant(s) to answer said summons at the place stated in the summons.

□ **NON EST**
Diligent search made and defendant ______ not to be found in the jurisdiction of this Court.

This [illegible] day of [illegible], 20[illegible].

DEPUTY

PLAINTIFF'S COPY

ID# 2023-0150687-CV
EFILED IN OFFICE
CLERK OF SUPERIOR COURT
COBB COUNTY, GEORGIA
23108528
~~Henry R. Thompson~~ - 68
OCT 31, 2023 11:55 AM
Connie Taylor, Clerk of Superior Court
Cobb County, Georgia

General Civil and Domestic Relations Case Filing Information Form

☑ Superior or □ State Court of Cobb County

For Clerk Use Only

Date Filed 10-31-2023
MM-DD-YYYY

Case Number 23108528

Plaintiff(s)					Defendant(s)				
Glenn, Ashley					Meta Platforms, Inc.				
Last	First	Middle I.	Suffix	Prefix	Last	First	Middle I.	Suffix	Prefix
Hood, Terrie									
Last	First	Middle I.	Suffix	Prefix	Last	First	Middle I.	Suffix	Prefix
Sorge, Kylie									
Last	First	Middle I.	Suffix	Prefix	Last	First	Middle I.	Suffix	Prefix
Hood, David									
Last	First	Middle I.	Suffix	Prefix	Last	First	Middle I.	Suffix	Prefix

Plaintiff's Attorney Lober, Michael Bar Number 455580 Self-Represented □

Check one case type and, if applicable, one sub-type in one box.

General Civil Cases

- □ Automobile Tort
- □ Civil Appeal
- □ Contract
- □ Contempt/Modification/Other Post-Judgment
- □ Garnishment
- □ General Tort
- □ Habeas Corpus
- □ Injunction/Mandamus/Other Writ
- □ Landlord/Tenant
- □ Medical Malpractice Tort
- □ Product Liability Tort
- □ Real Property
- □ Restraining Petition
- ☑ Other General Civil

Domestic Relations Cases

- □ Adoption
- □ Contempt
  - □ Non-payment of child support, medical support, or alimony
- □ Dissolution/Divorce/Separate Maintenance/Alimony
- □ Family Violence Petition
- □ Modification
  - □ Custody/Parenting Time/Visitation
- □ Paternity/Legitimation
- □ Support – IV-D
- □ Support – Private (non-IV-D)
- □ Other Domestic Relations

□ Check if the action is related to another action(s) pending or previously pending in this court involving some or all of the same parties, subject matter, or factual issues. If so, provide a case number for each.

_______________ Case Number _______________ Case Number

☑ I hereby certify that the documents in this filing, including attachments and exhibits, satisfy the requirements for redaction of personal or confidential information in O.C.G.A. § 9-11-7.1.

□ Is a foreign language or sign-language interpreter needed in this case? If so, provide the language(s) required.

_______________ Language(s) Required

□ Do you or your client need any disability accommodations? If so, please describe the accommodation request.

____

____

DISCLOSURE STATEMENT
CLERK OF SUPERIOR COURT

CASE NUMBER **23108528**

Glenn, Ashley; Hood, Terrie; Sorge, Kylie; Hood, David; Hood, Travis; Fratesi, Jennifer; Dean, Marya
Plaintiff

Vs.

Meta Platforms, Inc.;
Defendant

TYPE OF ACTION

- ○ Divorce without Agreement Attached
- ○ Divorce with Agreement Attached
- ○ Domestic Relations
- ○ Damages Arising out of Contract
- ☑ Damages Arising out of Tort
- ○ Condemnation
- ○ Equity
- ○ Zoning – County Ordinance Violations (i.e., Injunctive Relief-Zoning)
- ○ Zoning Appeals (denovo)
- ○ Appeal, Including denovo appeal – excluding Zoning
- ○ URESA
- ○ Name Change
- ○ Other
- ○ Recusal
- ○ Adoption

PREVIOUS RELATED CASES

Does this case involve substantially the same parties, or substantially the same subject matter, or substantially the same factual issues, as any other case filed in this court (Whether pending simultaneously or not)?

☑ NO
○ YES – If yes, please fill out the following:

1. Case # ____________________

2. Parties ____________________

3. Assigned Judge _____________

4. Is this case still pending? ○ Yes ○ No

5. Brief description of similarities:

/S/ **Lober, Michael**
Attorney or Party Filing Suit

SUPERIOR COURT OF COBB COUNTY
STATE OF GEORGIA

CIVIL ACTION NUMBER 23108528

$214.00 COST PAID

Glenn, Ashley
Hood, Terrie
Sorge, Kylie
Hood, David
Hood, Travis
Fratesi, Jennifer
Dean, Maryann
Mullholand, Michael
Brock, Carey
Eason, Haden
Ford, Matthew
Ford, Sherri
Mullholand, Spencer
Clark, Payton
Gleichman, Peter
Palmer, Margaret
Palmer, Ashley

PLAINTIFF

VS.

Meta Platforms, Inc.

DEFENDANT

SUPERIOR COURT OF COBB COUNTY
STATE OF GEORGIA

SUMMONS

TO: META PLATFORMS, INC.

You are hereby summoned and required to file with the Clerk of said court and serve upon the Plaintiff's attorney, whose name and address is:

Michael Lober
Lober & Dobson, LLC
1197 Canton St.
Roswell, Georgia 30075

an answer to the complaint which is herewith served upon you, within 30 days after service of this summons upon you, exclusive of the day of service. If you fail to do so, judgment by default will be taken against you for the relief demanded in the complaint.

This 31st day of October, 2023.

Clerk of Superior Court

COBB COUNTY
Georgia
1833
SUPERIOR COURT CLERK

Connie Taylor, Clerk of Superior Court
Cobb County, Georgia

IN THE SUPERIOR COURT OF COBB COUNTY

STATE OF GEORGIA

ASHLEY GLENN, TERRIE HOOD,)
KYLIE SORGE, DAVID HOOD,)
TRAVIS HOOD, JENNIFER FRATESI,)
MARYANN DEAN, MICHAEL)
MULLHOLAND, CAREY BROCK,) Plaintiff's Request a Jury Trial
HADEN EASON, MATTHEW FORD,)
SHERRI FORD, SPENCER)
MULLHOLAND, PAYTON CLARK,) CIVIL ACTION FILE NO.:
PETER GLEICHMAN,)
MARGARET PALMER, and)
ASHLEY PALMER)
)
)
Plaintiffs,)
v.)
)
META PLATFORMS, INC.,)
)
Defendant.)
)

COMPLAINT

Come now the Plaintiffs, who alleges the following facts and asserts the following causes of action against the Defendant, Meta Platforms, Inc., the entity formerly known as Facebook.

PARTIES, JURISDICTION & VENUE

1. Plaintiff Ashley Glenn is an adult resident citizen at 3962 Fairington Drive, Marietta, GA 30066 of Cobb County, the State of Georgia.

1. Plaintiff Terrie Hood is an adult resident citizen of the State of Georgia.

1. Plaintiff Kylie Sorge is an adult resident citizen of the State of Georgia.

1. Plaintiff David Hood is an adult resident citizen of the State of Georgia.

1. Plaintiff Travis Hood is an adult resident citizen of the State of Georgia.

1. Plaintiff Jennifer Fratesi is an adult resident citizen of the State of Georgia.

1. Plaintiff Maryann Dean is an adult resident citizen of the State of Georgia.

1. Plaintiff Michael Mullholand is an adult resident citizen of the State of Georgia.
1. Plaintiff Carey Brock is an adult resident citizen of the State of Georgia.
1. Plaintiff Haden Eason is an adult resident citizen of the State of Georgia.
1. Plaintiff Matthew Ford is an adult resident citizen of the State of Georgia.
1. Plaintiff Sherri Ford is an adult resident citizen of the State of Georgia.
1. Plaintiff Spencer Mullholand is an adult resident citizen of the State of Georgia.
1. Plaintiff Payton Clark is an adult resident citizen of the State of Georgia.
1. Plaintiff Peter Gleichman is an adult resident citizen of the State of Georgia.
1. Plaintiff Margaret Palmer is an adult resident citizen of the State of Georgia.
1. Plaintiff Ashley Palmer is an adult resident citizen of the State of Georgia.

2. Defendant Meta Platforms, Inc. (hereinafter "Meta" and/or "Facebook") is a corporation organized under the laws of the State of Delaware and which conducts business in this County and throughout Georgia. Its principal office is located in Menlo Park, California. Its registered agent for service in Georgia is Corporation Service Company, 2 Sun Court, Suite 400, Peachtree Corners, GA 30092. Meta is the same corporate entity that was initially known as Facebook, Inc. for many years, and changed its corporate name to Meta Platforms, Inc. in 2022. Meta is a publicly traded corporation and its common shares trade under the ticker symbol "META". Meta has a company value, or market capitalization, of more than $750 Billion, and has an average trading volume of more than 23 million common shares per day.

3. The events giving rise to the claims made the basis of this lawsuit arise from each Plaintiff's personal use of their personal internet connected devices, including their cell phone devices. Each Plaintiff's use of their personal internet connected devices, including their cell phone devices have regularly taken place in the State of Georgia.

4. The facts in this case are consistent with the claims in the class action case titled In re: Facebook Consumer User Profile Litigation, which was filed in 2018. (Case No. 3:18-md-

02843, N.D.Cal.). On October 11, 2023 the class action court issued an Order allowing each named Plaintiff to opt-out of a proposed settlement in the N.D.Cal. class action court. Each Plaintiff now files their individual claims as ordered and allowed by the class action court. The statute of limitations for each Plaintiff's claims has been tolled since the filing of the first class action complaints in 2018.

5. The amount in controversy for each named Plaintiff does not exceed $74,000.00, exclusive of interest and costs.

STATEMENT OF THE FACTS

Introduction

6. This is a Complaint about years-and-years of Meta and Facebook's corporate abuse and multiple lies to its customers and public regulators. The goal of Meta's lies was to get ahead in a competitive Silicon Valley social media money-making frenzy. The corporate abuses alleged herein are outrageous and among the worst in the history of American privacy rights. Plaintiffs are Facebook users that each have ownership of their cell phone internet-connected devices and/or other personal internet-connected hardware devices. Each Plaintiff maintains custody of their internet-connected device in Georgia. Defendant Facebook relies on Plaintiffs to operate their Georgia-based cell phones and hardware devices to "download" or otherwise allow Defendant to place its software onto the Plaintiff's device; i.e. an "App". Without Plaintiffs' hardware device, Defendant would have no means of distributing its software product known as "Facebook". In order to convince the Plaintiffs and other users to download Facebook, Meta has made representations about the Plaintiff's property/data contained on their personal devices, and representations that the Plaintiffs and other users have the ability to control access and distribution of property and data when using "Facebook". This Complaint contains allegations that show that

Meta's privacy settings were a misrepresentation to the Plaintiffs.

Facebook Changed the Default Privacy Settings from 2010-2014 to Make More Content Public, Prompting Federal Trade Commission Action.

7. Meta's business model is based on a user downloading its software, and then finding "Friends" on Facebook with whom to "connect". In doing so, Meta and Facebook made representations that the users, here the Plaintiffs, could decide the disbursement of their information, for example to keep among the user's chosen "Friends" or other "Privacy Settings". On Facebook, the Plaintiffs and other users chose who to add as their Friends. Hence, the electronic "social network" is created by each Plaintiff clicking/typing on their hardware device or tap-typing on their cell phone, at the location where the Plaintiff is located.

7. Users who signed up before November 2009 were assured that in general their content was nonpublic because Facebook's default Privacy Settings made most user content available only to Friends and Networks. For example, Friends had access to a user's Contact Information, Birthday, and other Profile Information, while Friends and Networks had access to Wall Posts, Photos, and Friends Lists. Only a user's name and network were designated as public information by Facebook. Users could control access to other content and information including Name, Profile Picture, Gender, Friend List, Pages, Networks, and Posts through Privacy Controls, as described in more detail elsewhere in this Complaint.

8. In December 2009, however, Facebook represented to users that it changed its Privacy Policy to designate additional items of user information as public. (See FTC Complaint, ¶20-22). With these changes, Facebook allegedly unilaterally made users' name, profile picture, gender, current city, Friend List and Page Likes public, regardless of a users' prior Privacy Settings. This meant that users at that time could not prevent other users or third-party Apps from seeing this content, including content that they had designated private. For users who had signed up and built a community on Facebook, their only choice was to leave Facebook or surrender their preferred privacy restrictions on some of their content and information. This was a breach of Facebook's promise to users that they controlled their content and information.

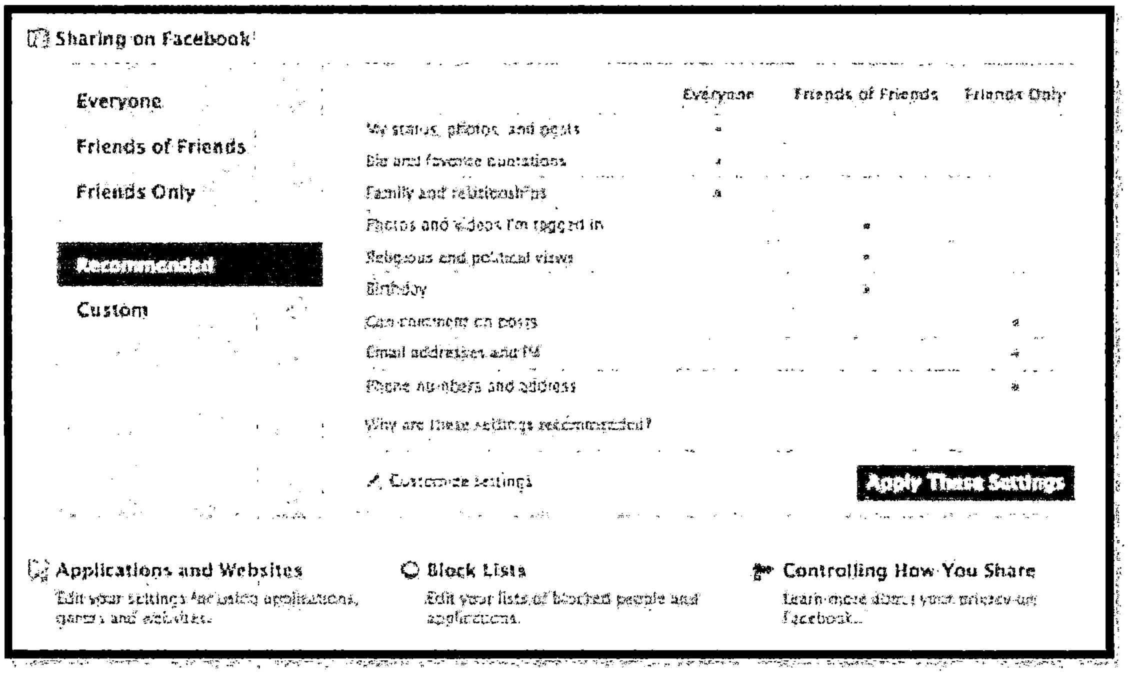
9. At that time, Facebook changed the default Privacy Settings for most other types of information, including for "About Me" information, Family and Relationships, Work and Education, and Posts, to "Everyone," changing the default of Photos and Videos, Birthday, and Religious and Political Views to Friends of Friends, and keeping access to user Contact Information to Friends Only.

10. However, even during this time period, users could privately message one another, reasonably expecting that content shared through Facebook Messenger would remain between those limited audiences. Users could also post and designate their post content private.

11. While the 2009 default Privacy Setting remained in place for new users until 2014, Facebook responded to the public outcry about the unilateral changes to public in May 2010, by representing to users that it would designate less user information as public. After May 26, 2010, a user's name, profile picture (should a user choose to have one), gender (though this could be hidden on the profile), and networks (should the user join any) were designated as PAI, and while current city, Friend List and Page Likes were defaulted to public, they could be changed by a user to a more private setting. (See Facebook, *Facebook Redesigns Privacy*, *supra* note 14.)

12. In May 2014, after years of controversy, Facebook represented to users that it restored the default Privacy Setting of"Friends Only" for Posts for new users, but did not change settings for existing users. (Josh Constine, *Facebook Stops Irresponsibly Defaulting Privacy of New Users' Posts to "Public," Changes to "Friends,"* TechCrunch (May 22, 2014), https://techcrunch.com/2014/05/22/sometimes- less-open-is-more.). Rather, Facebook offered existing users "Privacy Check-ups" that continued to recommend public disclosure of nearly all user content and information. Facebook also made the setting for posts "sticky," meaning that new posts defaulted to whatever setting was selected for the previous post. These user-content default settings have largely remained in place since 2014, though Facebook has made adjustments to the location and availability of privacy settings and controls. (Daniel Terdiman, *Facebook Just Announced These Changes To Try To Ease Your Mind On Privacy And Data*, Fast

Company (Mar. 28, 2018) https://www.fastcompany.com/40550689/how-facebook-is- striving-to-ease-userss-minds-on-privacy-and-data). Notably absent from Facebook's "Sharing Recommendations" seen below, is that the privacy settings fail to contain any selection for choices of sharing with any of Facebook's third-parties or Business Partners.



Sharing on Facebook

Everyone
Friends of Friends
Friends Only
Recommended
Custom

	Everyone	Friends of Friends	Friends Only
My status, photos, and posts	●		
Bio and favorite quotations	●		
Family and relationships	●		
Photos and videos I'm tagged in		●	
Religious and political views		●	
Birthday		●	
Can comment on posts			●
Email addresses and IM			●
Phone numbers and address			●

Why are these settings recommended?

Customize settings

Apply These Settings

Applications and Websites
Edit your settings for using applications, games and websites.

Block Lists
Edit your lists of blocked people and applications.

Controlling How You Share
Learn more about your privacy on Facebook.

Facebook Allowed Third Parties to Access Facebook Users' Content and Information Without or Beyond the Scope of Users' Consent.

13. Through its use of various API technology, Facebook allowed App Developers, device makers, and other Business Partners to access its platform and interact with Facebook users. For example, Facebook used an "Events API" to allow users to grant an App permission to get information about events the user is hosting or attending, including private events. Additionally, Facebook used a "Groups API" to make it easier for users to post and respond to content in their groups. Likewise, Facebook offered a "Pages API" to help App Developers create tools for Page owners to schedule posts and reply to comments or messages.

14. In April 2018, following the Cambridge Analytica Scandal and resulting inquiries,

Facebook acknowledged that all three of these APIs could provide access to a great deal of user content and information and, thus, Facebook opted to impose more requirements for App Developers before they could gain access to user data through any of these APIs.

15. Facebook's Graph API, is the "primary way to get data into and out of the Facebook platform." (*Overview—Graph API*, Facebook for Developers, https://developers.facebook.com/docs/graph- api/overview (last visited Feb. 20, 2019). The first version of Graph API, Graph API v1.0, available from April 2010 to May 2015, was very permissive. (*Changelog—Graph API*, Facebook for Developers, https://web.archive.org/web/20141208030452/https://developers.facebook.com/docs/apps/changelog# (last visited on Feb. 20, 2019). It was ultimately through this platform that Cambridge Analytica purchased the data of as many as 87 million Facebook users.

Facebook Developed an Interface That Allowed App Developers to Access a Facebook User's Content and Information Via That User's Friend.

16. Graph API v1.0 enabled the App Developers to access and store the App User's name, gender, birthdate, location, photos, and Page likes. App Developers could also collect this information from the App User's Friends. Device makers and Business Partners had similar access.

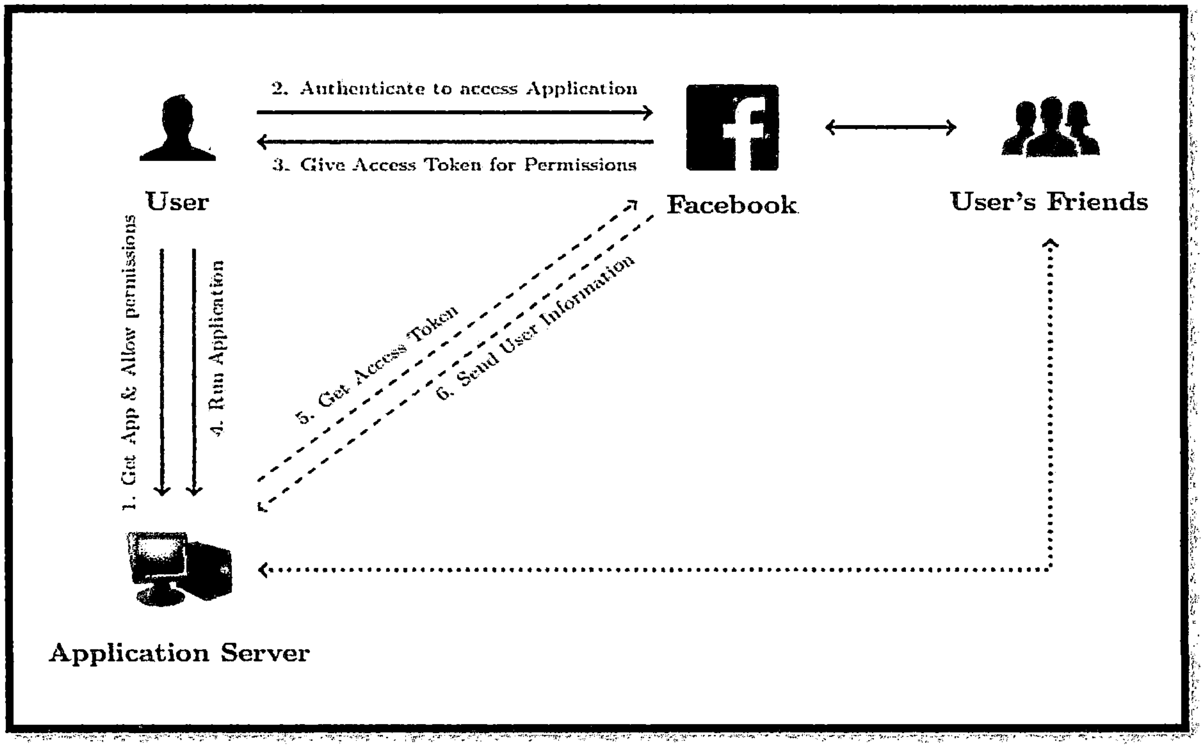
17. Facebook organizes users' content and information on Graph API as "objects" (Also referred to as "nodes." *Overview—Graph API, supra)* (e.g., people, photos, events, and pages), "connections" between users (Also referred to as "edges." *Id.*) (e.g., Friend relationships, shared content, and photo tags), and fields which is the metadata associated with an object.

18. Metadata, or "data about data," are additional pieces of data associated with each Post, message, or other content. Metadata provides context to data. For example, the metadata of a video includes the timestamp of when the video was created, the profile of the user who created the video, and the title and description of the video. Facebook metadata also include users'

privacy restrictions. When Facebook made certain user content, such as photos and videos, available on Graph API v1.0, the metadata reflecting user's privacy designations associated with this content was not provided to third parties, although other metadata was.

19. In order to read, publish, and delete non-public content and information on Graph API v1.0, App Developers needed to request permission from the user that downloaded and logged into the application.

20. For every permission that is granted, Facebook grants a corresponding "access token," that the App Developer can then use to query information though the Graph API. After the App Developer submits the query, Graph API returns that object as well as a set of metadata and connections associated for that object.



21. Third parties using the Graph API v1.0 could access user-data in two ways: server-based and browser-based.

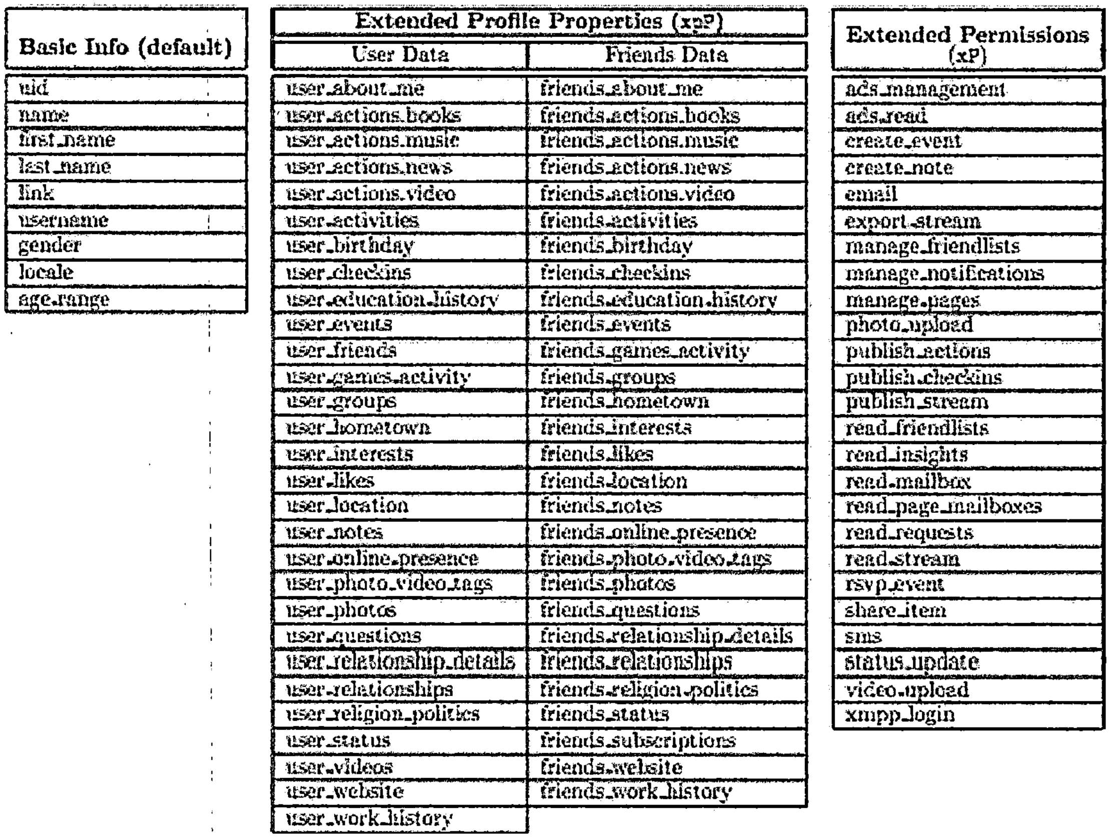
22. Through the server-based method, a user installs the App, which then allows the App to get an "access token" from Facebook. Once the App receives an access token, it may use it to issue a request for certain user data (or Friend data) to Facebook's server. Facebook will respond by transmitting the requested data to the App server. The data contained in Facebook's response is then received and stored by the App server.

23. The browser-based method is slightly different. A user installs the App, which then resides in the user's web browser. After installation, the App obtains an "access token" and, using the access token, may issue a request for certain user data (or Friend data) to Facebook's server. Facebook will respond by transmitting the requested data to the user's browser. The App sends this data from the user's browser to the App server, which stores it.

24. In the browser-based method, Facebook's server sends data to the user's browser. Unknown to Facebook or the user, the App code, which resides in the user's browser, captures this data before it reaches the user and sends it to the App's own server. Thus, it is plausible to consider it an interception. In the server-based method, on the other hand, Facebook's server sends data to the App's server, so that an App residing in the user's browser cannot intercept it.

25. In both server-based and browser-based methods, third parties were able to store users' content and information.

26. Under Graph API v1.0, App Developers could access different categories of users' content and information. The graph below displays all categories of information available under Graph API v1.0:



Basic Info (default)
uid
name
first_name
last_name
link
username
gender
locale
age_range

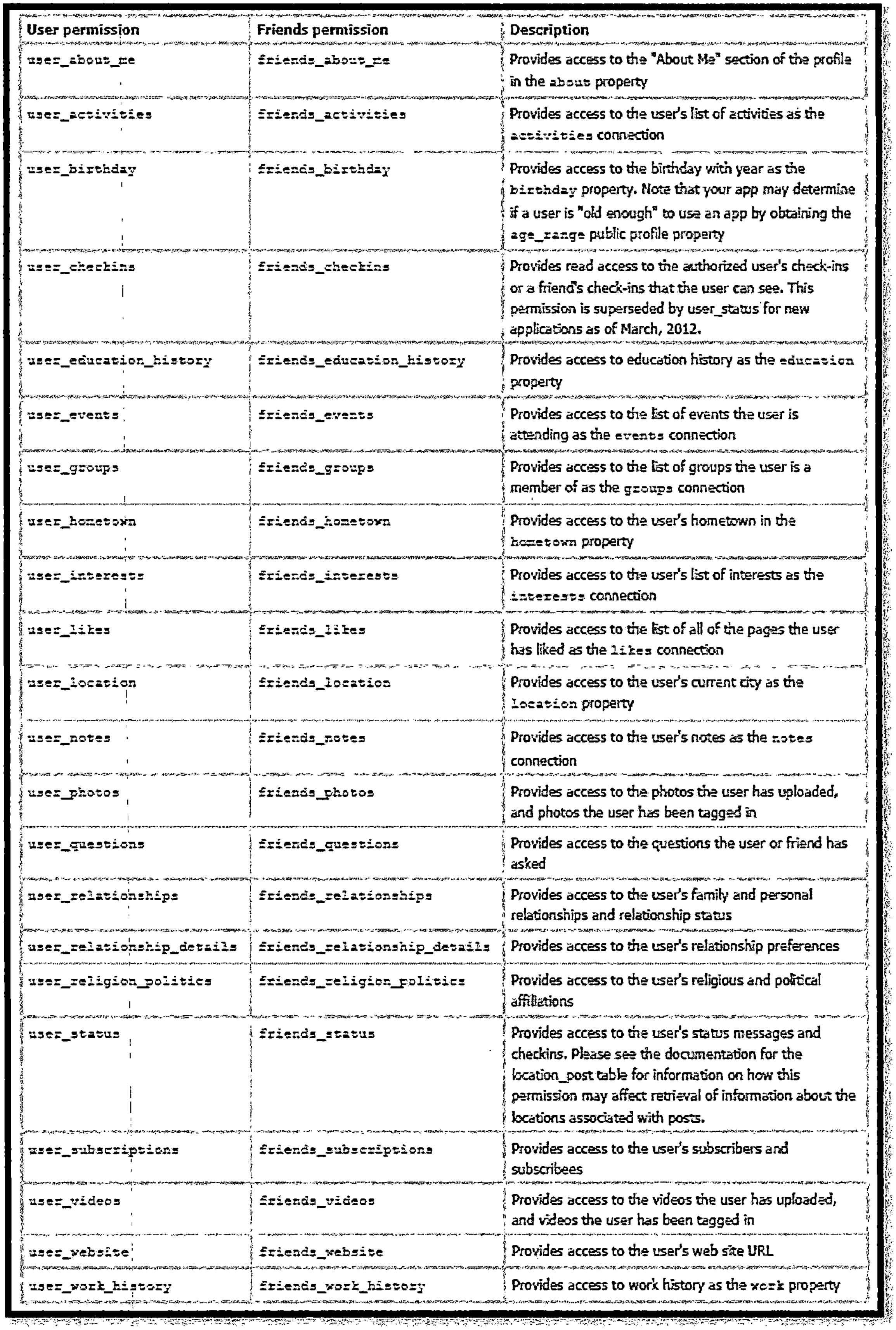
Extended Profile Properties (xpP)	
User Data	Friends Data
user_about_me	friends_about_me
user_actions.books	friends_actions.books
user_actions.music	friends_actions.music
user_actions.news	friends_actions.news
user_actions.video	friends_actions.video
user_activities	friends_activities
user_birthday	friends_birthday
user_checkins	friends_checkins
user_education_history	friends_education_history
user_events	friends_events
user_friends	friends_games_activity
user_games_activity	friends_groups
user_groups	friends_hometown
user_hometown	friends_interests
user_interests	friends_likes
user_likes	friends_location
user_location	friends_notes
user_notes	friends_online_presence
user_online_presence	friends_photo_video_tags
user_photo_video_tags	friends_photos
user_photos	friends_questions
user_questions	friends_relationship_details
user_relationship_details	friends_relationships
user_relationships	friends_religion_politics
user_religion_politics	friends_status
user_status	friends_subscriptions
user_videos	friends_website
user_website	friends_work_history
user_work_history	

Extended Permissions (xP)
ads_management
ads_read
create_event
create_note
email
export_stream
manage_friendlists
manage_notifications
manage_pages
photo_upload
publish_actions
publish_checkins
publish_stream
read_friendlists
read_insights
read_mailbox
read_page_mailboxes
read_requests
read_stream
rsvp_event
share_item
sms
status_update
video_upload
xmpp_login

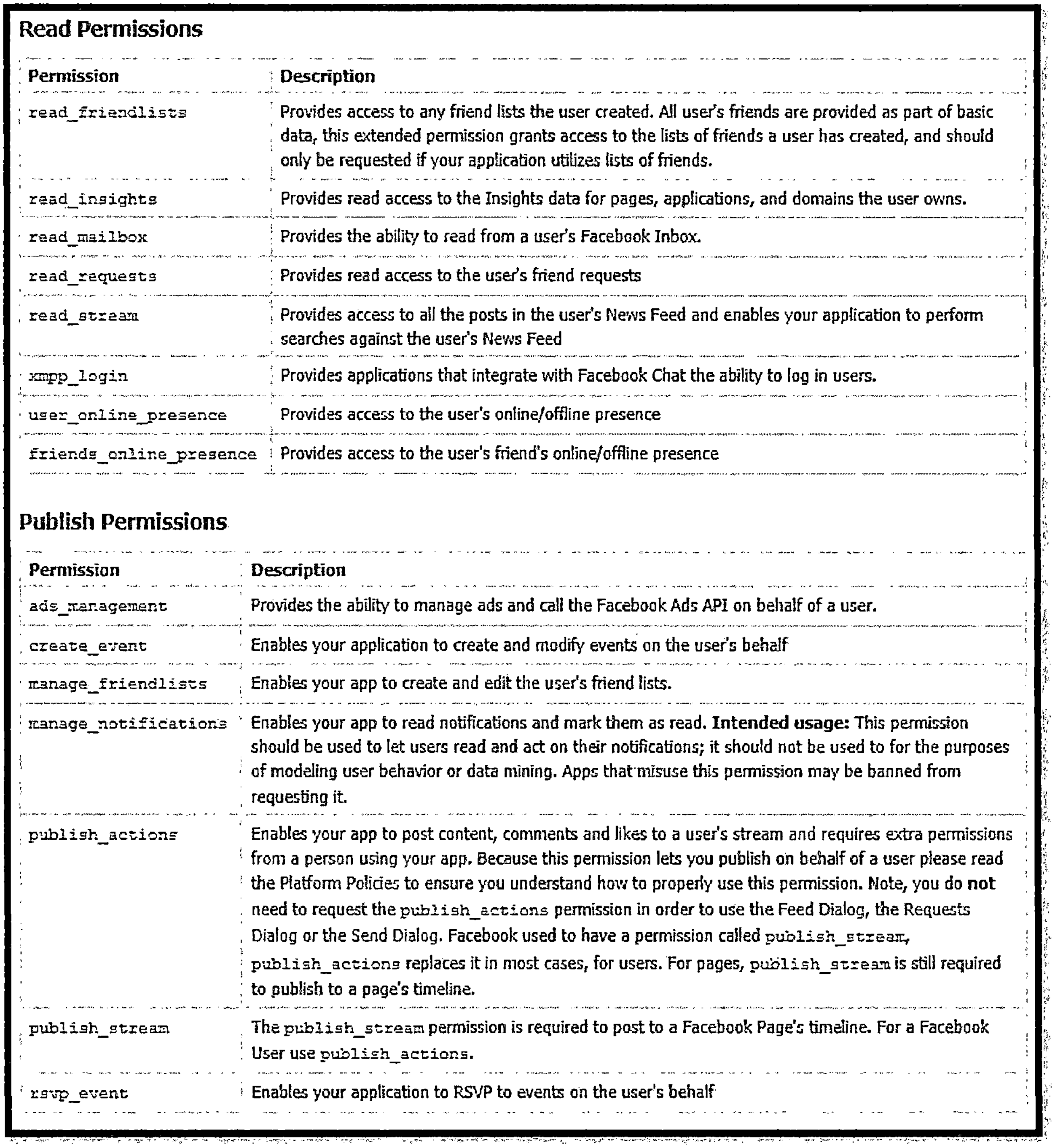
26. Under Graph API v1.0, App Developers, by default gained access to users' "Basic Info," which included their User ID, name, gender, their current city, age, Friend lists, and any other information that the App User had made publicly available. (See *Permissions Reference*, Facebook Developers, (Sept. 23, 2012), https://web.archive.org/web/20120923065901/https://developers.facebook.com/docs/authentication /per missions/ (last visited Feb. 20, 2019)). In order to gain access to nonpublic content and information, App Developers needed to request permission from the App User. Through this process, App Developers gained access to the App User's content and information and the user's Friends' content and information.

27. Under Graph API v1.0, App Developers could request three types of permissions: User permission, Friends permission, and Extended Permissions.[110]

28. Graph API v1.0 categorized both the User and Friends permissions as "Extended Profile Properties." Extended Profile Properties included: about me; activities; birthdays; check ins; education history; events; groups; hometown; interests; likes; location; notice; photos; questions; relationships; relationship details; religion and politics; status; subscriptions; videos; websites; and work history. A chart from Facebook's App Developer page defining these permissions follows below: (See *Extended Profile Properties*, Facebook Developers (Sept. 11, 2013), https://developers.facebook.com/docs/reference/login/extended-profile-properties/ [https://web.archive.org/web/20130911191323/https://developers.facebook.com/docs/reference/login/ext ended-profile-properties/].)



User permission	Friends permission	Description
user_about_me	friends_about_me	Provides access to the "About Me" section of the profile in the about property
user_activities	friends_activities	Provides access to the user's list of activities as the activities connection
user_birthday	friends_birthday	Provides access to the birthday with year as the birthday property. Note that your app may determine if a user is "old enough" to use an app by obtaining the age_range public profile property
user_checkins	friends_checkins	Provides read access to the authorized user's check-ins or a friend's check-ins that the user can see. This permission is superseded by user_status for new applications as of March, 2012.
user_education_history	friends_education_history	Provides access to education history as the education property
user_events	friends_events	Provides access to the list of events the user is attending as the events connection
user_groups	friends_groups	Provides access to the list of groups the user is a member of as the groups connection
user_hometown	friends_hometown	Provides access to the user's hometown in the hometown property
user_interests	friends_interests	Provides access to the user's list of interests as the interests connection
user_likes	friends_likes	Provides access to the list of all of the pages the user has liked as the likes connection
user_location	friends_location	Provides access to the user's current city as the location property
user_notes	friends_notes	Provides access to the user's notes as the notes connection
user_photos	friends_photos	Provides access to the photos the user has uploaded, and photos the user has been tagged in
user_questions	friends_questions	Provides access to the questions the user or friend has asked
user_relationships	friends_relationships	Provides access to the user's family and personal relationships and relationship status
user_relationship_details	friends_relationship_details	Provides access to the user's relationship preferences
user_religion_politics	friends_religion_politics	Provides access to the user's religious and political affiliations
user_status	friends_status	Provides access to the user's status messages and checkins. Please see the documentation for the location_post table for information on how this permission may affect retrieval of information about the locations associated with posts.
user_subscriptions	friends_subscriptions	Provides access to the user's subscribers and subscribees
user_videos	friends_videos	Provides access to the videos the user has uploaded, and videos the user has been tagged in
user_website	friends_website	Provides access to the user's web site URL
user_work_history	friends_work_history	Provides access to work history as the work property



Read Permissions

Permission	Description
read_friendlists	Provides access to any friend lists the user created. All user's friends are provided as part of basic data, this extended permission grants access to the lists of friends a user has created, and should only be requested if your application utilizes lists of friends.
read_insights	Provides read access to the Insights data for pages, applications, and domains the user owns.
read_mailbox	Provides the ability to read from a user's Facebook Inbox.
read_requests	Provides read access to the user's friend requests
read_stream	Provides access to all the posts in the user's News Feed and enables your application to perform searches against the user's News Feed
xmpp_login	Provides applications that integrate with Facebook Chat the ability to log in users.
user_online_presence	Provides access to the user's online/offline presence
friends_online_presence	Provides access to the user's friend's online/offline presence

Publish Permissions

Permission	Description
ads_management	Provides the ability to manage ads and call the Facebook Ads API on behalf of a user.
create_event	Enables your application to create and modify events on the user's behalf
manage_friendlists	Enables your app to create and edit the user's friend lists.
manage_notifications	Enables your app to read notifications and mark them as read. **Intended usage:** This permission should be used to let users read and act on their notifications; it should not be used to for the purposes of modeling user behavior or data mining. Apps that misuse this permission may be banned from requesting it.
publish_actions	Enables your app to post content, comments and likes to a user's stream and requires extra permissions from a person using your app. Because this permission lets you publish on behalf of a user please read the Platform Policies to ensure you understand how to properly use this permission. Note, you do **not** need to request the publish_actions permission in order to use the Feed Dialog, the Requests Dialog or the Send Dialog. Facebook used to have a permission called publish_stream, publish_actions replaces it in most cases, for users. For pages, publish_stream is still required to publish to a page's timeline.
publish_stream	The publish_stream permission is required to post to a Facebook Page's timeline. For a Facebook User use publish_actions.
rsvp_event	Enables your application to RSVP to events on the user's behalf

29. In addition, App Developers could request "Extended Permissions" from the App User. These permissions gave access to the content and information of both the App Users and the users' Friends.

These permissions are defined in the inserted screenshot. (*Extended Permissions*, Facebook Developers (Sept. 11, 2013), https://developers.facebook.com/docs/reference/login/extended-permissions/ [https://web.archive.org/web/20130911191422/https://developers.facebook.com/docs/reference/login/extended-permissions/].) Through these Facebook permissions, App Developers gained access to the content and information about the App User's Friends. For example, "Read_mailbox" permission allowed the App Developer to read the ***private*** messages of users. That unauthorized access would include messages sent to and from the App User's Friends.

30. Also, "read_stream" allowed the App Developer to read the nonpublic posts on the App User's timeline. This access would include content posted by the App User's Friends on the user's timeline even if that content was meant only for Friends. It also included any content that the App User's Friends had been tagged in. Tagging is a metadata field that refers to the process by which users can link other users to objects on Facebook.

31. App Developers sought all permissions, including the permissions that gave access to Friends' content and information, from the App User when she downloaded or logged into the App. Facebook did not send any notification to Friends when third party App developers gained these permissions.

32. Regarding Facebook's sharing of content and information with App Developers, Ashkan Soltani, independent researcher and consultant and former Chief Technologist at the Federal Trade Commission, stated that he "found that time and time again Facebook allows App Developers to access personal information of users and their Friends, in contrast to their privacy settings and their policy statements," and consequently "there is very little the user can do to prevent their information from being accessed." (DCMS Report, *supra* note 28 ¶ 89, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.).

Graph API Allows App Developers to Access Users' Video Information.

33. A key element of Apps, for users, was the ability to watch and share video content on

Facebook's platform. Facebook has developed considerable resources into collecting, curating and enabling users to watch videos on its platform.

34. To provide this functionality, Facebook stores video information in its data centers, and further stores copies of videos in secondary distribution centers known as "edge caches" located throughout the World. There are ten such distribution centers in the United States alone. When a user attempts to access videos on the Platform, Facebook sends out the copy of the video from the nearest distribution center. The viewer is then able to watch the video on Facebook. Facebook has successfully encouraged users to watch videos on the platform and video viewing is a substantial component of user activity on Facebook. In 2013, Facebook announced that it was "starting to test an easier way to watch videos on Facebook." (Brent Ayrey, *A New Way to Watch Videos from Facebook on Your TV*, Facebook Newsroom (Oct. 13, 2016), https://newsroom.fb.com/news/2016/10/a-new-way-to-watch-videos-from-facebook-on-your- tv/.)

35. A 2016 Facebook Newsroom post stated, "[w]e're focused on creating video experiences that people want, and we've heard that people want different options for how and where they watch videos that they discover on Facebook."[117] Facebook Watch, a feature released in 2017, touted Facebook's expanded video platform for "[o]riginal shows and popular videos." (Facebook Newsroom, *Introducing Watch, a New Platform for Shows on Facebook* (Aug. 9, 2017), https://newsroom.fb.com/news/2017/08/introducing-watch-a-new-platform-for-shows-on-facebook.)

36. Facebook, in turn, passed information about how users watched video content onto third parties. For example, video information was available to App Developers through at least seven different categories of data. These categories included: "users_videos", "friends_video"; "users_subscriptions"; "friends_subscriptions"; "users_likes"; "friends_likes"; and "read_stream". Facebook set users' default App settings to allow sharing of six out of the seven of these categories.

37. According to Facebook's definition, the data queries "users_videos" and "friends_video" permissions allowed App Developers to obtain "the videos the user has uploaded, and videos the user has been tagged in." Facebook set users' default "App settings" to allow all of this information to be shared with App Developers through a user's Friend. Thus, any App Developer who requested these permissions

could have received video information from all users who had not changed the default settings.

38. The "users_likes" and "friends_likes" data categories allowed access "to the list of all of the pages the user [had] liked." Facebook defines "Facebook Pages" as "a public profile that allows anyone including artists, public figures, businesses, brands, organizations, and charities to create a presence on Facebook and engage with the Facebook community."

39. According to Facebook's SEC S-1 filing in April 2012, "Examples of popular Pages on Facebook include Lady Gaga, Disney, and Manchester United, each of which has more than 20 million Likes." By March 31, 2012, "there were more than 42 million Pages with ten or more likes." Accordingly, users' likes would have included the Facebook pages for any movies, television shows, actors, production studios, etc., that the user had liked. Facebook set users' default "App settings" to allow this information to be shared to App Developers through a users' Friend.

40. Facebook allowed App Developers access to video information through the "read_stream" query. Facebook's Developer webpage defined this category as providing "access to all the posts in the user's News Feed and enables your application to perform searches against the user's News Feed." This information would include any videos uploaded by the user as well as any videos or video hyperlinks shared with a user. It would also include any and all posts by that user and any and all posts shared with that user about videos. For instance, an App Developer using this permission setting could see a user's posted critique of a specific movie.

41. Facebook also allowed access through "read_mailbox" category of information, which allowed Developers were able to read the private messages between the App User and her Friends. Thus, if users shared videos through messenger, the App Developer would gain access to users' video information. This permission was removed from Facebook's APIs in October 2015. (*Changelog*, Facebook for Developers, https://developers.facebook.com/docs/graph- api/changelog/archive (last visited Feb. 21, 2019).

42. Information made available to Apps and third parties about what video users viewed and what they posted about the videos, is a rich source of content and information for Facebook with

tremendous value.

To Allow Third Parties Unauthorized Access to Users' Content and Information, Facebook Stripped Users' Privacy Designations for Certain Content Available on Graph API.

43. The investigations following the Cambridge Analytica scandal have revealed that Facebook's platform *actually removed user privacy designations* from some of the content provided to third parties. This is significant in light of Facebook's strenuous representations, in the Class Action court and around the world, that users' privacy settings were honored. Investigation of counsel in the California Class Action case has further revealed violations of users' privacy settings not previously publicly described as a finding of any other investigation.

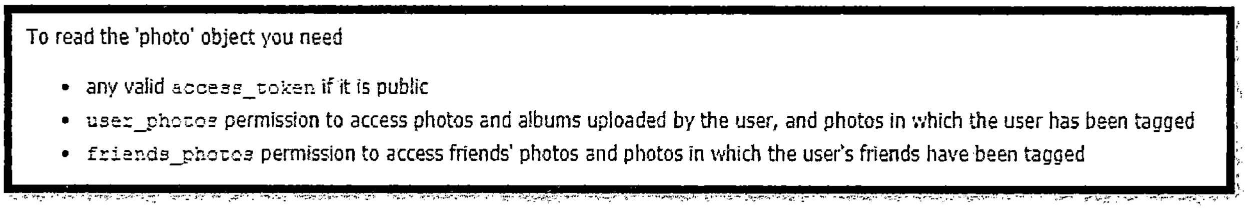
44. Facebook misrepresented that it provided users tools to limit the audiences who could view the content they shared on a per-post basis. These post-based privacy selections were available regardless of default settings. For example, a user with "public" default settings could still elect to post something and limit the audience to something more private such as "Friends." Alternatively, that user might send a photo in a private message via Facebook Messenger. Facebook misrepresented to users unequivocally that those settings would be honored.

45. Both the default and per-post-based privacy designations are metadata associated with content on Facebook. For example, when a video is posted, the video metadata includes the timestamp of when the video was created, the profile of who created the video, and any comment associated with that video. However, during at least part of the Class Period, when Facebook made certain content – including Photos, Videos, Checkins, and Status –available on Graph API v1.0, the metadata reflecting user's privacy designations associated with this content was not provided to third parties, even though other metadata was.

46. Because Facebook fraudulently induced the Plaintiffs and stripped privacy designation metadata from the associated content, third parties were unable to verify that a user's privacy settings allowed for this content to be shared and, therefore, could not confirm that they were adhering to users' privacy designations as required by Facebook's SRR. (*Statement of Rights and Responsibilities*, Facebook (June 8, 2012), www.facebook.com/legal/terms, [https://web.archive.org/web/20121205191915/https://www.facebook.com/legal/terms)

47. From at least 2010 to present, Facebook has maintained a Developer Webpage that provides

an overview of Graph API. The Developer Webpage includes the permission required to access an object, the metadata fields of that object, and the connections associated with that object. For example, in 2012, the top of the Photo webpage demonstrated the following permissions that may be required to view the photo: (See *Photo*, Facebook Developers (Oct. 18, 2012), http://developers.facebook.com/docs/reference/ api/photo/ [https://web.archive.org/web/20121018125458/http://developers.facebook.com/ docs/reference/api/photo/].)

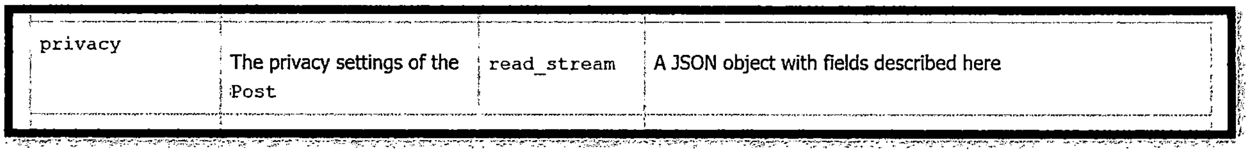


To read the 'photo' object you need

- any valid `access_token` if it is public
- `user_photos` permission to access photos and albums uploaded by the user, and photos in which the user has been tagged
- `friends_photos` permission to access friends' photos and photos in which the user's friends have been tagged

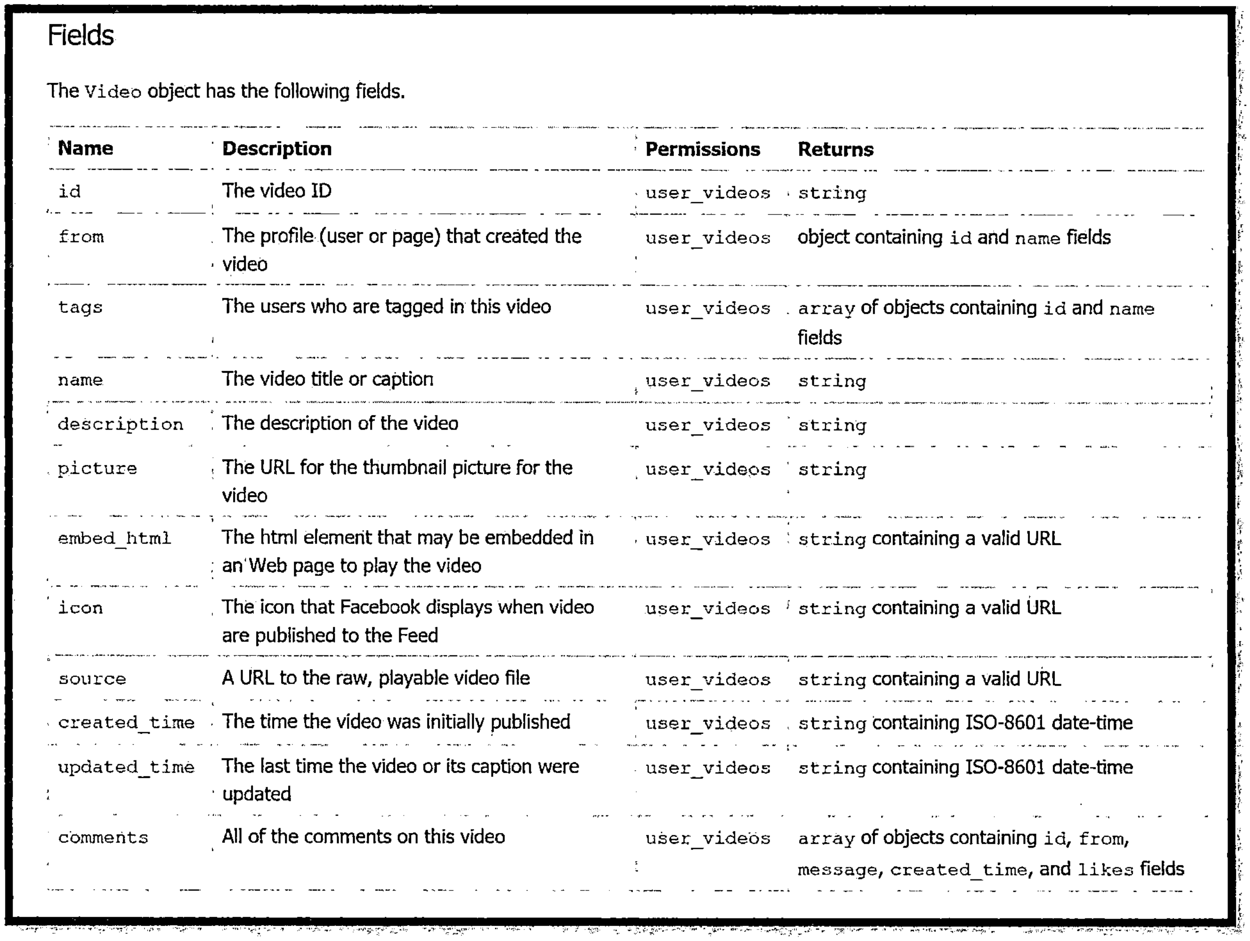
48. As shown above, certain permissions were required when App Developers sought access to non-public information on Graph API. The Webpage also displays the metadata fields associated with each object. In 2012, for example, the fields for photographs included: ID, From, Tags, Name, Name_tags, Icon, Picture, Source, Height, Width images, Link, Place, Created_time, Updated_time, Position. *Photo*, Facebook Developers (Oct. 18, 2012), http://developers.facebook.com/docs/reference/ api/photo/ [https://web.archive.org/web/20121018125458/http://developers.facebook.com/ docs/reference/api/photo/].) However, from at least 2010 to 2013, Facebook did not include the privacy restriction metadata in the fields listed for certain objects, such as photos and videos.

49. Yet, Facebook did include privacy restriction metadata for other objects, such as Events, Groups, and Posts. For example, the Facebook webpage for Posts includes the privacy restriction metadata under fields. A screenshot follows below: (See *Post*, Facebook Developers (Nov. 9, 2013), https://developers.facebook.com/docs/reference/api/post/ [https://web.archive.org/web/20131109050811/https://developers.facebook.com/docs/reference/api/post/].)



`privacy`	The privacy settings of the `Post`	`read_stream`	A JSON object with fields described here

50. Notably, Facebook included the privacy metadata on some objects following the shift to Graph API v2.0 in May 2015. For example, Videos did not include the privacy restriction metadata in 2010 to 2013; however, in 2015, Facebook's Developer Webpage began including the privacy metadata for Videos. As shown on the data insert here below, from September 18, 2013, the Developer Webpage displayed the following fields available for Video objects, which does not include privacy restriction metadata: (*Video*, Facebook Developers (May 29, 2013), http://developers.facebook.com/docs/reference/api/video/ [https://web.archive.org/web/20130529165931/http://developers.facebook.com/docs/reference/api/video/].)

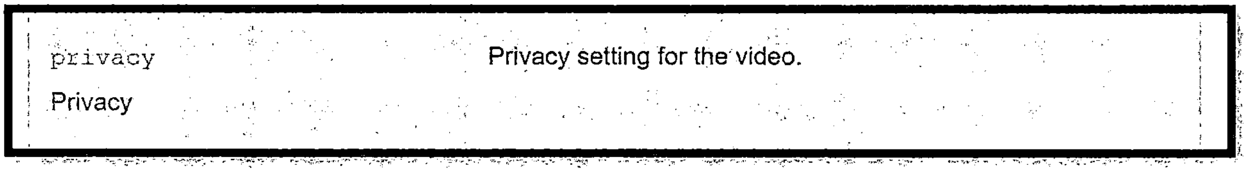


Fields

The `Video` object has the following fields.

Name	Description	Permissions	Returns
`id`	The video ID	`user_videos`	`string`
`from`	The profile (user or page) that created the video	`user_videos`	object containing `id` and `name` fields
`tags`	The users who are tagged in this video	`user_videos`	`array` of objects containing `id` and `name` fields
`name`	The video title or caption	`user_videos`	`string`
`description`	The description of the video	`user_videos`	`string`
`picture`	The URL for the thumbnail picture for the video	`user_videos`	`string`
`embed_html`	The html element that may be embedded in an Web page to play the video	`user_videos`	`string` containing a valid URL
`icon`	The icon that Facebook displays when video are published to the Feed	`user_videos`	`string` containing a valid URL
`source`	A URL to the raw, playable video file	`user_videos`	`string` containing a valid URL
`created_time`	The time the video was initially published	`user_videos`	`string` containing ISO-8601 date-time
`updated_time`	The last time the video or its caption were updated	`user_videos`	`string` containing ISO-8601 date-time
`comments`	All of the comments on this video	`user_videos`	`array` of objects containing `id`, `from`, `message`, `created_time`, and `likes` fields

51. Yet, by November 5, 2015, the Developer Webpage included Privacy setting in its list of fields associated with Video objects: (See *Video*, Facebook Developers (Nov. 5, 2015), http://developers.facebook.com/docs/reference/ api/video/ [https://web.archive.org/web/20151105092521/https://developers.facebook.com/docs/graph-api/reference/video].)



`privacy` Privacy	Privacy setting for the video.

52. Because Facebook stripped privacy restrictions metadata from the associated content, third

parties were unable to verify that a user's privacy settings allowed for this content to be shared and, therefore, could not confirm that they were adhering to users' privacy settings as required by Facebook's Platform Policy. Upon information and belief, Facebook alone was responsible for determining what content was loaded into Graph API v1.0. The removal of users' privacy metadata from certain content including photos and videos, persisted from at least 2010-2013.

53. Facebook's stripping of the privacy metadata was a deliberate act unknown to users, that thwarted users' affirmative privacy designations as to photos and videos by allowing third parties to access users' content without providing users' corresponding privacy settings. Thus, Facebook failed to provide third parties with the crucial information that would have allowed third-party Apps to verify that they were accessing users' photos in compliance with users' privacy settings.

54. With regard to Apps, these actions are Facebook's fraudulent inducement and a misrepresentation to users. Namely, "[w]e require applications to respect your privacy…." (See *Statement of Rights and Responsibilities*, Facebook (June 8, 2012), https://www.facebook.com/ legal/terms [https://web.archive.org/web/20121205191915/https://www.facebook.com/legal/terms]). Upon information and belief, Facebook was notified by at least one App Developer, of the missing metadata associated with photos and the subsequent inability of the App Developer to verify that it was adhering to users' privacy designations as early as 2012.

55. Upon information and belief, Facebook deliberately allowed App Developers to access users' photos and videos, without regard to their privacy settings, in order to maximize the amount of user content and information available to third parties. Indeed, if the metadata containing privacy designations had been made available through Graph API v1.0, it would have greatly diminished App Developers' ability to use this content. The failure to provide this metadata served Facebook's plan for growth-at-all-costs. That is, here as elsewhere, Facebook's actual practice undermined the policy to which it paid lip service, egregiously harming users and greatly benefiting Facebook.

Cambridge Analytica Used Facebook's "Graph API Interface" to Take Users' Content and Information.

56. In 2007, psychologists Michal Kosinski and David Stillwell from Cambridge University's Psychometrics Centre began using a Facebook quiz they developed called "myPersonality" to study

personality traits of consenting users. The App determined gender, age and sex, opening doors for psychologists to consider different ways to connect "likes" with personality traits. Their research received notice from the U.S. Defense Advanced Research Projects Agency ("DARPA"). Kosinski and Stillwell published their findings in the Proceedings of the National Academy of Sciences in 2013. (See Eric Killelea, *Cambridge Analytica: What We Know About the Facebook Data Scandal*, Rolling Stone (Mar. 20, 2018) https://www.rollingstone.com/culture/culture-news/cambridge-analytica-what- we-know-about-the-facebook-data-scandal-202308/).

57. Researchers from Cambridge University used the "myPersonality" quiz to create a database "with profile information for over six million Facebook users. It has those users' psychological profiles, their likes, their music listening, their religious and political views, and their locations, among other information. It says it can predict users' leadership potential, personality, and 'satisfaction with life.'"(Kashmir Hill, *The Other Cambridge Personality Test Has Its Own Database with Millions of Facebook Profiles*, Gizmodo (Mar. 22, 2018), https://gizmodo.com/the-other-cambridge-personality- test-has-its-own-databa-1823997062.)

58. In 2013, Cambridge Analytica approached the myPersonality App team to get access to the App's data but was turned down because of its political ambitions. Only after the Cambridge Analytica Scandal did Facebook reveal that data from myPersonality had been publicly available for years. (Phee Waterfield & Timothy Revell, *Huge new Facebook data leak exposed intimate details of 3M users*, New Scientist (May 15, 2018).

59. In 2013, Aleksandr Kogan and his company Global Science Research ("GSR") created an application called "MyDigitalLife" (also known as "thisisyourdigitallife"). Facebook had begun collaborating with Kogan concerning Facebook data in 2012. The agreement that Kogan struck with Facebook in 2013 allowed Kogan to launch the MyDigitalLife App on the Facebook platform. (Eric Killelea, *Cambridge Analytica: What We Know About the Facebook Data Scandal*, Rolling Stone (Mar. 20, 2018) https://www.rollingstone.com/culture/culture-news/cambridge-analytica-what- we-know-about-the-facebook-data-scandal-202308/)

60. Facebook's ties with GSR run deep. One of GSR's two co-founders, Joseph Chancellor, was

an employee at Facebook before 2018, but was placed on administrative leave after the Cambridge Analytica Scandal was publicized in 2018.

61. MyDigitalLife marketed itself to Facebook users as a tool that would help them have a better understanding of their own personalities, and that would supply data for use by academic psychologists. The App prompted users to answer questions for a psychological profile. Questions focused on the so-called "Big Five" personality traits: extraversion, agreeableness, openness, conscientiousness, and neuroticism.

62. Through MyDigitalLife, Kogan initially gained access to the personal data of the approximately 300,000 Facebook users that downloaded the App. In spring 2014, Kogan was approached by an SCL- affiliated contractor and was asked to provide consulting services. Kogan set up GSR to carry out the work. The project was intended to deliver to SCL personality scores matched to the voter registration file for several million people. Kogan authorized GSR's Facebook App to collect data from App users about not just the user, but also the user's Friends. This data was then used to predict personality and then provided back to SCL.

63. GSR made no secret of the blatantly commercial nature of its use of Facebook data. It states in its "End User Terms and Conditions" that it intended to "sell" and "license (by whatever means and on whatever terms)" the personal content it obtained through the YDL App. Facebook was provided with GSR's terms of service and thus was given constructive if not actual notice that GSR was selling user content and information. Kogan has stated that he "never heard a word" from Facebook concerning his intent to "sell" data even though he had publicly posted his intention for a year and a half.

64. Kogan and GSR actively began their relationship with Cambridge Analytica in 2014 and 2015. During this time, Kogan and GSR provided Cambridge Analytica with much more than the personal content and information of the Facebook users who had downloaded the MyDigitalLife App. Graph API v1.0, which Facebook was still using, allowed the App to access the data that users' *Friends* had shared with them, even though the Friends had not used the App. Through this platform, Facebook gave Kogan and GSR, and thus Cambridge Analytica and other third parties like the University of Toronto and the University of British Columbia, the content and information of more than 50 million additional people,

mostly Americans.

65. Facebook in 2018 represented that, of the up to 87 million Facebook users affected by the scheme, only approximately 300,000 of them had downloaded the MyDigitalLife App—and those users had agreed to share only their own content and information for the limited purposes associated with the App. Facebook admitted, however, that its historical logs of users' privacy settings are scant. Upon information and belief, at least the photos shared with Cambridge Analytica were stripped of information that would have communicated the privacy restrictions of users' Friends.

66. In addition to supplying Cambridge Analytica with fresh Facebook user data on an ongoing basis, Kogan and GSR, at Cambridge Analytica's request, also performed modelling work on the data. Communications disclosed by Cambridge Analytica personnel demonstrate Kogan's active role in this modeling.

67. CEO Zuckerberg has admitted that Facebook became aware that Kogan and GSR had misused data in 2015 and conducted an investigation. (See *Facebook's Use and Protection of User Data: Hearing Before the H. Energy and Commerce Comm.*, 2018 WL 1757479, at 22-23 (Apr. 11, 2018) (Statement of Mark Zuckerberg). AT that time, Facebook did not disclose its internal investigation to the Plaintiffs. Defendant Facebook states that it contacted Kogan following the publication of the *Guardian* article in 2015. The 2015 report from the *Guardian* was thus focused on U.K. citizens and did not receive any meaningful media attention in the United States.

68. At a minimum, Facebook became aware as early as the 2015 *Guardian* news actions that GSR sold Facebook data containing personal content of American citizens. Further, by March 2016, when, while negotiating a settlement of claims with Kogan, Facebook was informed that Kogan had made roughly $800,000 re-selling Facebook user data. Facebook failed to determine at that time the scope and extent of the content and information GSR had obtained. Indeed, Facebook waited over two years until 2018 to make any type of public disclosure. (The Plaintiff's actions in the instant case have been tolled since the 2018 Plaintiff class action case was initially filed, and the opt-out order was issued in September 2023).

69. Kogan initially used the Facebook data that he had obtained in 2012 and subsequently to co-author a number of papers that had obvious commercial purposes and applications. Kogan co- authored papers entitled "*Tracing Cultural Similarities and Differences in Emotional Expression through Digital*

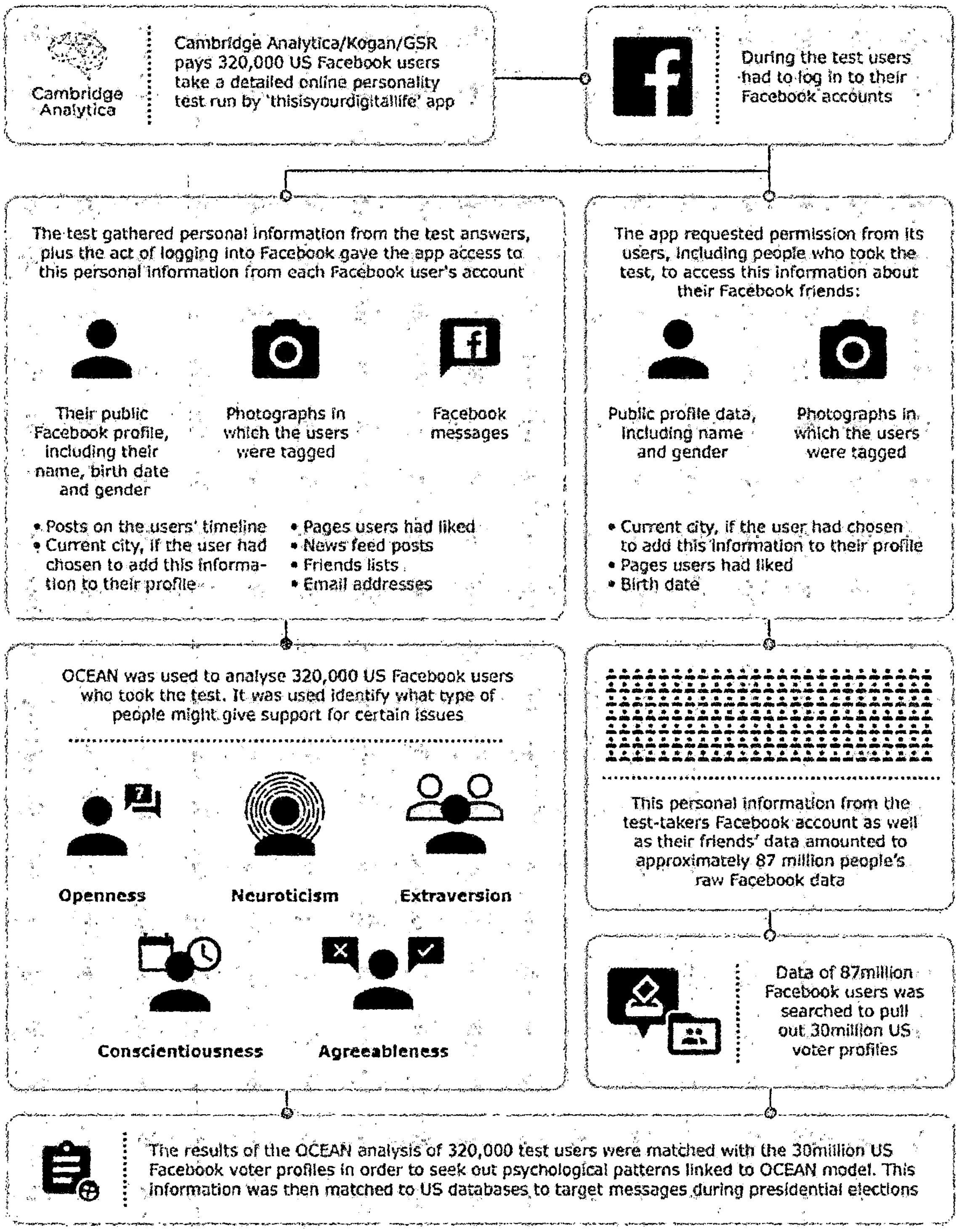
Records of Emotions," "*Happiness Predicts Larger Online Social Networks for Nations and Individuals Low, but not High, in Consumeristic Attitudes and Behaviors,*" "*Silk Road to Friendships: Economic Cooperation is Associated with International Friendships around the World,*" "*Big Data Public Health: Online Friendships can Identify Populations At-Risk of Physical Health Problems and All-Causes Morbidity,*" and "*Donations Predict Social Capital Gains for Low SES, But Not High SES Individuals and Countries.*" (See Def. Facebook, Inc.'s Resps. & Objs. to Pls.' First Set of Interrogs. at pp. 7-8 (Sept. 7, 2018, Class Action Discovery).

70. Christopher Wylie, a former Cambridge Analytica contractor, has recently revealed how the data mining process at Cambridge Analytica worked: By getting access to Facebook users' "profiles, likes, even private messages, [Cambridge Analytica] could build a personality profile on each person and know how best to target them with messages."(See Forbes article, Parmy Olson, *Face-To-Face With Cambridge Analytica's Elusive Alexander Nix*, Forbes (Mar. 20, 2018), https://www.forbes.com/sites/parmyolson/2018/03/20/face-to-face-with-cambridge-analytica- alexander-nix-facebook-trump/#54972c48535f). Facebook users' profiles "contained enough information, including places of residence, that [Cambridge Analytica] could match users to other records and build psychographic profiles."(See Matthew Rosenberg, et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump- campaign.html). Mr. Wylie has said: "We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on." (See Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, The Guardian (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.)

71. The figure below was created by the United Kingdom Information Commissioner's Office ("ICO"), which is a government agency set up to uphold information rights in the public interest, and to promote openness by public bodies and data privacy for individuals. The figure describes how Cambridge Analytica accessed and harvested the content and information of millions of Facebook users: (See *Investigation Into the Use of Data Analytics in Political Campaigns – Investigation Update*, (July 11, 2018),

Information Commissioner's Office, ("ICO Report") at 17, https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf.). The flowchart set forth on the page below demonstrates how Facebook and Cambridge Analytica gained personal information from the personal internet devices of 87 million people without the consent of those people, and used the information to influence election activity:

Data harvesting of the Facebook data



Cambridge Analytica/Kogan/GSR pays 320,000 US Facebook users take a detailed online personality test run by 'thisisyourdigitallife' app

During the test users had to log in to their Facebook accounts

The test gathered personal information from the test answers, plus the act of logging into Facebook gave the app access to this personal information from each Facebook user's account

Their public Facebook profile, including their name, birth date and gender
Photographs in which the users were tagged
Facebook messages

- Posts on the users' timeline
- Current city, if the user had chosen to add this information to their profile
- Pages users had liked
- News feed posts
- Friends lists
- Email addresses

The app requested permission from its users, including people who took the test, to access this information about their Facebook friends:

Public profile data, including name and gender
Photographs in which the users were tagged

- Current city, if the user had chosen to add this information to their profile
- Pages users had liked
- Birth date

OCEAN was used to analyse 320,000 US Facebook users who took the test. It was used identify what type of people might give support for certain issues

This personal information from the test-takers Facebook account as well as their friends' data amounted to approximately 87 million people's raw Facebook data

Data of 87million Facebook users was searched to pull out 30million US voter profiles

The results of the OCEAN analysis of 320,000 test users were matched with the 30million US Facebook voter profiles in order to seek out psychological patterns linked to OCEAN model. This information was then matched to US databases to target messages during presidential elections

72. As outlined above, the British ICO found that GSR obtained the following

information from users who downloaded the MyDigitalLife App:

> Public Facebook profile, including their name and gender; Birth date; Current city, if the user had chosen to add this information to their profile; Photographs in which the users were tagged; Pages that the users had liked Posts on the users' timelines; News feed posts; Friends lists; Email addresses; and Facebook messages. (See United Kingdom ICO Report, at 19-20)

73. The ICO reports that GSR obtained the following information from the App Users' Friends: "Public profile data, including their name and gender; Birth date; Current city if the friends had chosen to add this information to their profile; Photographs in which the friends were tagged; and Pages that the friends had liked. (See United Kingdom ICO Report, at p. 20).

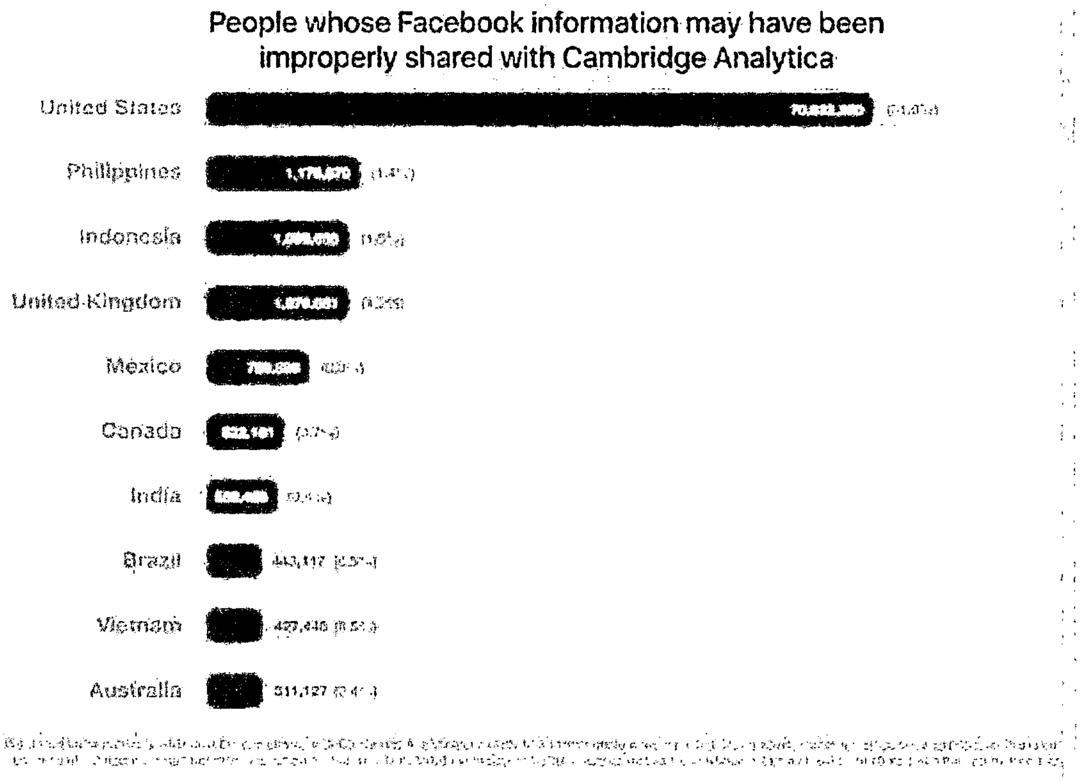
74. GSR obtained access to users' and users' Friends likes. (See United Kingdom ICO Report, at p. 20). This information would include specific video information about these users. GSR shared this like information with Cambridge Analytica. (*see also* U.K. House of Commons, Digital, Culture, Media and Sport Committee, Testimony of Dr. Aleksandr Kogan (Apr. 24, 2018), at Q1930,http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital -culture- media-and-sport-committee/ fake-news/oral/81931.html). Thus, Facebook allowed GSR to access and share the specific video preferences of its users through this "likes" information.

75. Through Facebook's breach of its user's privacy, GSR obtained access to the "posts on the users' timelines" for users who installed the MyDigitalLife App. (See United Kingdom ICO Report, at p. 20). This access would have been available from Facebook under the "read_stream" query. Facebook initially falsely denied that it denied Aleksandr Kogan's request to access this query.(See Def. Facebook, Inc.'s Resps. & Objs. to Pls.' First Set of Interrogs. at pp. 6-7, class action discovery ("Dr. Kogan's App Review application sought extended permissions for the App . . . Facebook rejected Dr. Kogan's application the next day, stating that the App would not be using the data requested to enhance the user's in-app experience.")). But Facebook's interrogatory response contradicts the U.K.'s ICO's published report on this matter. Through this query, GSR obtained additional access to any information about a user's video

preferences posted on that user's timeline.

76. Only after the Cambridge Analytica Scandal became public through media reports in March 2018, did Facebook announce that it was suspending Cambridge Analytica and its parent company, Strategic Communication Laboratories ("SCL"), from Facebook.

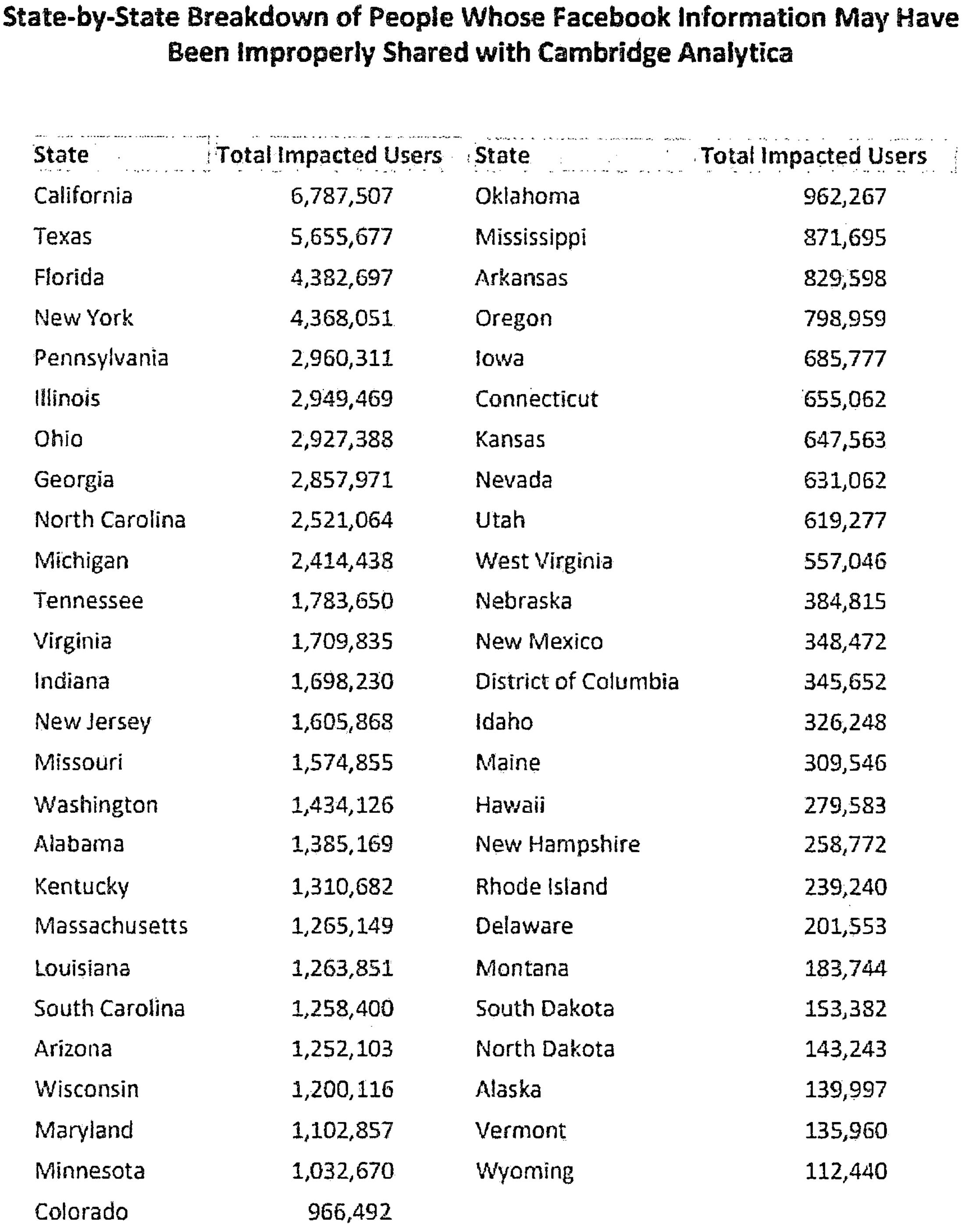
77. On April 4, 2018, Facebook released the following statement: "In total, we believe the Facebook information of up to 87 million people—mostly in the United States—may have been improperly shared with Cambridge Analytica." Facebook also released a country-by-country breakdown of the millions of users affected by the GSR App, pictured below:



(See Mike Schroepfer, Facebook, *An Update on Our Plans to Restrict Data Access on Facebook*, Facebook Newsroom (Apr. 4, 2018), https://newsroom.fb.com/news/2018/04/restricting-data-access/)

78. Plaintiffs could not have discovered Facebook's action prior to the April 4, 2018 "newsroom" release. However, even on April 4, 2018, Facebook did not disclose the full range

of its data privacy failures to the public. On May 1, 2018, Facebook updated this blog post to include a state-by-state breakdown of the millions of American users who may have had their information shared with Cambridge Analytica. Facebook admitted in the blog post that over 2.8 million Georgia residents had their personal data and information sent to Cambridge Analytica, as shown in the graph on the page below:



State-by-State Breakdown of People Whose Facebook Information May Have Been Improperly Shared with Cambridge Analytica

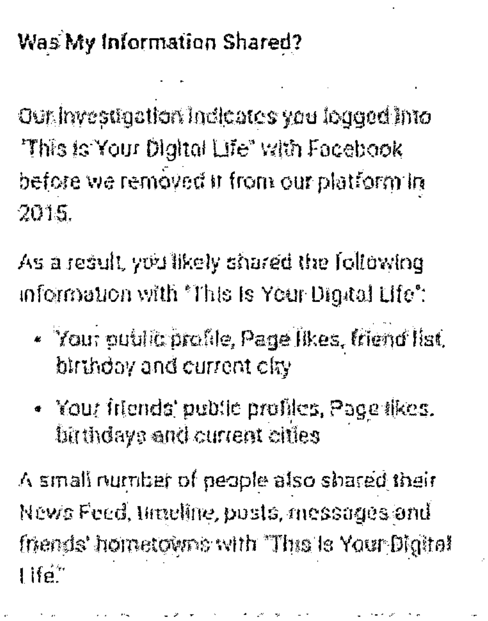
State	Total Impacted Users	State	Total Impacted Users
California	6,787,507	Oklahoma	962,267
Texas	5,655,677	Mississippi	871,695
Florida	4,382,697	Arkansas	829,598
New York	4,368,051	Oregon	798,959
Pennsylvania	2,960,311	Iowa	685,777
Illinois	2,949,469	Connecticut	655,062
Ohio	2,927,388	Kansas	647,563
Georgia	2,857,971	Nevada	631,062
North Carolina	2,521,064	Utah	619,277
Michigan	2,414,438	West Virginia	557,046
Tennessee	1,783,650	Nebraska	384,815
Virginia	1,709,835	New Mexico	348,472
Indiana	1,698,230	District of Columbia	345,652
New Jersey	1,605,868	Idaho	326,248
Missouri	1,574,855	Maine	309,546
Washington	1,434,126	Hawaii	279,583
Alabama	1,385,169	New Hampshire	258,772
Kentucky	1,310,682	Rhode Island	239,240
Massachusetts	1,265,149	Delaware	201,553
Louisiana	1,263,851	Montana	183,744
South Carolina	1,258,400	South Dakota	153,382
Arizona	1,252,103	North Dakota	143,243
Wisconsin	1,200,116	Alaska	139,997
Maryland	1,102,857	Vermont	135,960
Minnesota	1,032,670	Wyoming	112,440
Colorado	966,492		

79. In his April 2018 testimony to the U.K. House of Commons, Facebook Chief Technology Officer Mike Schroepfer testified that Facebook did not read terms and conditions of any Developer's Apps that were put on Facebook. (*See* U.K. House of Commons, Digital,

Culture, Media and Sport Committee, Testimony of Mike Schroepfer (Apr. 26, 2018), at Q2141, http://data.parliament.uk/writtenevidence/committeeevidence.svc/ evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake- news/oral/82114.pdf). In the user privacy class action litigation, in its interrogatory responses, Facebook has averred that it could not possibly have read the terms and conditions of these Apps, because there were millions of them. (See Def. Facebook, Inc.'s Resps. & Objs. to Pls.' First Set of Interrogatories in the privacy class action litigation, at p. 20). This is one more indication that Facebook did not protect user content and information once it gave access to App Developers.

80. On April 9, 2018, with a notification at the top of News Feeds, Facebook began notifying individual users of the "This is Your Digital Life" App that their data had been shared with Cambridge Analytica. The notification from Facebook in April 2018 stated that the user had logged into "This is Your Digital Life" and the public profile, page likes, friend list, birthday, current city, friend's public profiles, friends' page likes, friends' birthdays, and friends' current cities were likely shared with "This is Your Digital Life." The notification also explained that a small number of people also shared their News feed, timeline, posts, messages, and friends' hometowns with "This is Your Digital Life."

81. Upon information and belief, Facebook failed to send the notification to all Georgia Facebook users whose data had been breached, and instead only sent messages to the Digital Life App login users. Upon information and belief, the App login user's notification looked like this below:



Was My Information Shared?

Our investigation indicates you logged into "This is Your Digital Life" with Facebook before we removed it from our platform in 2015.

As a result, you likely shared the following information with "This is Your Digital Life":

- Your public profile, Page likes, friend list, birthday and current city
- Your friends' public profiles, Page likes, birthdays and current cities

A small number of people also shared their News Feed, timeline, posts, messages and friends' hometowns with "This is Your Digital Life."

82. On April 22, 2018, Dr. Kogan finally broke his silence in an interview with CBS News Correspondent Lesley Stahl on 60 Minutes. Kogan stated he had terms of service up on his application for a year and a half—terms providing that he could sell the Facebook data he obtained through the App—and yet Facebook never enforced its agreement with Kogan or its rules against selling data during this time. Kogan also explained that the ability to gather people's Facebook Friends' data without their permission was a Facebook core feature, available to anyone who was a Developer. He explained that there are likely tens of thousands of applications that did what he did, as this was not a bug, but a feature of which Facebook was aware.

The Cambridge Analytica Scandal Has Triggered Additional Revelations of the Facebook Apps' Misuse of User Content and Information.

83. Following the news reports of the Cambridge Analytica Scandal, Facebook conducted its own internal audit into other App Developers, but has not made the details public, with scant exception. Audit reports prepared by PricewaterhouseCoopers have been heavily redacted. Nonetheless, it is known that millions of Apps had access to users' data

prior to Facebook's 2014 platform changes. Facebook has now admitted that it has suspended not less than 400 of the App Developers "due to concerns around the Developers who built them or how the information people chose to share with the app may have been used." Facebook's review appears to have been limited to Apps that had access to user content and information prior to 2014, when Facebook changed its platform policies. On March 21, 2018, Mr. Zuckerberg took to Facebook to acknowledge Facebook's breach of trust, while Ms. Sandberg acknowledged that Facebook allowed Apps to access more user content and information than necessary.

84. In a March 21, 2018 Facebook post, CEO Mark Zuckerberg acknowledged a "breach of trust between Facebook and the people who share their data with us and expect us to protect it" and said, "We need to fix that."(See Mark Zuckerberg, Facebook (Mar. 21, 2018), https://www.facebook.com/zuck/posts/10104712037900071.). His post stated that in addition to investigating Cambridge Analytica, Facebook was also investigating "all Apps that had access to large amounts of information.". *Id.* Facebook did not notify the Plaintiffs that their personal data and property had been breached. CEO Zuckerberg repeated the same sentiment in full-page ads in several British and American newspapers a few days later.

85. Also on March 21, 2018, Facebook Executive Sheryl Sandberg posted to her Facebook account that Facebook is "taking steps to reduce the data [Facebook users] give an app" when they use their Facebook account, and the Company intends to "make it easier" for users to have a better understanding of which Apps they have "allowed to access [their] data." (See Lila MacLellan, *Sheryl Sandberg wants you to know she regrets Cambridge Analytica*, Quartz at Work (Mar. 21, 2018), https://qz.com/work/1234977/facebook-coo-sheryl-sandberg-is-finally-speaking- out-about-cambridge-analytica/).

86. However, it appears that Facebook made these statements only to assuage public outcry and prevent users from leaving the platform and to placate regulators until

attention died down. Facebook's attempts to distance itself from these statements when called to account in this lawsuit should not be countenanced.

87. Further, in the wake of the Cambridge Analytica Scandal, Facebook suspended two other companies from its platform in April 2018 for improper data collection: Canadian consulting firm AggregateIQ and CubeYou.

88. On or about April 6, 2018, Facebook suspended AggregateIQ, who played a pivotal role in the Brexit campaign, from the platform, following reports it may be connected to Cambridge Analytica's parent company, SCL. This was nearly three (3) years after Facebook learned of Cambridge Analytica's psychographic marketing. On or about April 8, 2018, Facebook suspended the CubeYou App from the platformafter CNBC notified them that CubeYou had misled users by collecting data from quizzes inaccurately labeled "non-profit academic research" and then selling the findings to marketers, and had business ties to Cambridge Analytica.

89. Facebook announced the suspension of hundreds of other Apps, but has not provided disclosure of the additional detail on those suspensions, including the sale and misuse of user content and information.

Facebook Also Enabled Device Makers and Other Business Partners to Access Users' Content and Information Through Friends.

90. Facebook partnered with a diverse set of companies, including Business Partners, to develop and integrate Facebook's User Platform on multiple devices and operating systems. As part of these agreements, Facebook gave Business Partners access to Plaintiffs and other users' content and information. Facebook created private APIs (i.e. computer programming codes) to secretly transfer Plaintiffs and users' content and information to these Business Partners. Facebook has identified 53 of their Business Partners. Those companies include:

- Accedo
- Acer

- Airtel
- Alcatel / TCL
- Alibaba
- Amazon
- Apply
- AT&T
- Blackberry
- Dell
- DNP
- Docomo
- Garmin
- Gemalto
- HP / Palm
- HTC
- Huawei
- INQ
- Kodak
- LG
- MediaTek / Mstar
- Microsoft
- Miyowa / Hape Esia
- Motorola / Lenovo
- Mozilla
- Myriad
- Nexian
- Nokia
- Nuance
- O2
- Opentech ENG
- Opera Software
- OPPO
- Orange
- Pantech
- PocketNet
- Qualcomm
- Samsung
- Sony
- Sprint
- T-Mobile
- TIM
- Tobii
- U2topia

- Verisign
- Verizon
- Virgin Mobile
- Vodafone
- Warner Bros.
- Western Digital
- Yahoo
- Yandex[152]
- Zing Mobile

91. Facebook notes that this list is "comprehensive to the best of our ability." However, it further stated that "[i]t is possible we have not been able to identify some integrations, particularly those made during the early days of our company when our records were not centralized. It is also possible that early records may have been deleted from our system."(*See* Letter from Facebook, Inc. to Chairman Greg Walden, Ranking Member Frank Pallone, Energy & Commerce Committee, and U.S. House of Representatives, *Facebook's Response to House Energy and Commerce Questions for the Record* at 22 (June 29, 2018) https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM- 20180411.pdf.

92. Facebook formed certain Business Partnerships related to sharing user data as early as 2007. These deals allowed Facebook to expand its reach by outsourcing to Business Partners the time, labor and money required to build Facebook's Platform on different devices and operating systems. In exchange, Facebook allowed these Business Partners to access users' content and information. Facebook partnered with a diverse set of companies including foreign internet device makers, such as Blackberry and Huawei, and other types of internet companies, such as Chinese internet company Alibaba, Yahoo, and Russian technology company Yandex. Facebook allowed users' content and information to be accessed by "tens of millions of mobile devices, game consoles, televisions and other

systems" that were not in Facebook's direct control. (*See* Gabriel J.X. Dance, et al., *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, N.Y. Times (June 3, 2018), https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends- data.html).

93. These partnerships were built in part on "data reciprocity." Facebook and its partners agreed to exchange information about American users' activities, including to technology companies in countries that have openly conflicted with the interests of the United States. This was not disclosed to users or the Plaintiffs.

94. Like Apps, the content and information that the Business Partners accessed varied. As on Graph API, Business Partners gained access not only TO the content and information of the user who downloaded or used the Facebook service that the Business Partner provided, but also to the content and information of the user's Friends. (*Id.* see Gabriel J.X. Dance, et al., N.Y. Times) Sandy Parakilas, a whistleblower and a former operations manager at Facebook, asserts that the same "feature" is behind both the Cambridge Analytica Scandal and Facebook's data sharing with device makers. In both cases, "developers had access" to a user's Friend data. (See Sandy Parakilas (@mixblendr), Twitter (June 4, 2018, 12:44 AM), https://twitter.com/mixblendr/status/1003542895507501057)(See also The Guardian, Paul Lewis, *Utterly Horrifying: ex-Facebook Insider Says Covert Data Harvesting Was Routine*, March 20, 2018). Parakilas stated in the report: "It has been painful watching because I know that they could have prevented it" and that he told executives they should "audit developers directly and see what's going on with the data" and that one executive said "do you really want to see what you'll find?" (*Id.*, The Guardian 3/20/2018). In his statements, Parakilas equated device makers to "apps." For instance, Blackberry, had access to the App User's messages and other personal information of the App User's Friends, such as their political and religious preferences, education and work history, events they plan to attend, and whether they were currently online. (*Id.* see Gabriel J.X. Dance, et al., N.Y. Times). On November 20, 2017, A Facebook executive wrote a memorandum posted for the news media again

representing to the public and the Plaintiff that Facebook was then protecting the user's property. (See John Osofsky, VP Global Operations, *Enforcing Our Policies and Protecting People's Data*, November 20, 2017. https://about.fb.com/news/h/enforcing-our-policies-and-protecting-peoples-data/)

95. A team of Investigative journalists at the New York Time reported that some of the Business Partners, like Yahoo, were able to read the streams of users' and users' Friends posts, while others, like Sony, Microsoft and Amazon, were able to obtain the users' and users' Friends emails. (See Gabriel J.X. Dance, Michael LaForgia, and Nicholas Confessore, *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. Times (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html.)

96. Facebook also gave Business Partners access to the unique Facebook identifiers of users, ("Facebook ID") including the user's Friends, and the user's Friends' Friends ("Friends of Friends"). For instance, Blackberry had access as recently as 2017 to the unique Facebook identifiers of Blackberry users', users' Friends, and users' Friends of Friends. Facebook knew or should have known that its actions would damage its users; even The Wall Street Journal reported on the dangers associated with providing third parties Facebook users' unique ID many years earlier in October 2010. (See Emily Steel and Geoffrey A. Fowler, *Facebook in Privacy Breach*, Wall Street Journal (Oct. 18, 2010), https://www.wsj.com/articles/SB10001424052702304772804575558484075236968 ("The apps reviewed by the Journal were sending Facebook ID numbers to at least 25 advertising and data firms, several of which build profiles of Internet users by tracking their online activities."). In that same 2010 article, the Journal reported that Facebook represented that it would stop giving this information to third parties due to privacy concerns: "A Facebook user ID may be inadvertently shared by a user's Internet browser or by an application," the [Facebook] spokesman said. Knowledge of an ID "does not permit access to anyone's private information on Facebook," he said, adding that the company would introduce new technology

to contain the problem identified by the Journal. (See Emily Steel and Geoffrey A. Fowler, *Facebook in Privacy Breach*, Wall Street Journal (Oct. 18, 2010), https://www.wsj.com/articles/SB10001424052702304772804575558484075236968 ("The apps reviewed by the Journal were sending Facebook ID numbers to at least 25 advertising and data firms, several of which build profiles of Internet users by tracking their online activities.")

97. In May 2015, Facebook again failed to act when it recognized the need for an even more secure way to process IDs, and switched to "unique App IDs" whereby each App is now given a unique App ID. (See *Facebook Application Development FAQ*, Facebook for Developers, https://developers.facebook.com/docs/apps/faq/ (last visited February 21, 2019)

98. Despite the acknowledged risks of providing users' Facebook ID to third parties, Facebook continued giving Business Partners, such as BlackBerry and Yandex, access to this information.

Facebook Extended Certain "Whitelisted" Companies Access to Friends' Information Despite Facebook's Contrary Representations to Users.

99. Following the FTC inquiry, at Facebook's f8 Developers' conference in April 2014, Facebook represented to the public that it was restricting access to user content and information by cutting off third parties' ability to download information via Graph API v1.0 and stated it would give App Developers one year, or until May 2015, to continue accessing Friends' information. (See *f8 2014: Stability for Developers & More Control for People*, Facebook Newsroom (Apr. 30, 2018), https://newsroom.fb.com/news/2014/04/f8-2014-stability-for-developers-and-more-control-for-people- in-apps/). Mark Zuckerberg announced "we are going to make it so now everyone has to choose to share their own data with an app themselves." (See Larry Magid, *Zuckerberg Pledges More User Control of Facebook App Privacy –Unveils Anonymous Log-In*, Forbes (Apr. 30, 2014), https://www.forbes.com/sites/larrymagid/2014/04/30/zuckerberg- pledges-more-user-control-of-app-privacy-unveils-anonymous-log-in/#7bea50036de7). Facebook unveiled its new theme

"putting people first" and stated, "We are giving people more control over these experiences so they can be confident pressing the blue button."(*Id. see f8 2014: Stability for Developers & More Control for People*, Facebook Newsroom (Apr. 30, 2018)).

100. Likewise, on April 28, 2015, Facebook's Simon Cross commented on the transition to a more restrictive Graph API stating, "[I]f people don't feel comfortable using Facebook and specifically logging in [to] Facebook and using Facebook in apps, we don't have a platform, we don't have developers." (See Josh Constinue, *Facebook Is Shutting Down Its API for Giving Your Friends' Data to Apps*, TechCrunch (Apr. 28, 2015), https://techcrunch.com/2015/04/28/facebook-api-shut-down/). Cross further told the reporter that the privacy changes were the result of Facebook's self-styled "People First" goal, which the facts now show was a misnomer.

101. However, Facebook did not disclose that, while restricting Graph API v1.0 for general third parties, Facebook allowed certain companies to continue accessing content and information of users and users' Friends. This special access, termed "whitelisting," allowed Apps to "access user data without permission" and "to circumvent users' privacy [or] platform settings and access Friends' information, even when the user disabled the Platform." (See DCMS Report, *supra*). To facilitate whitelisting, Facebook developed and promulgated "Private Extended APIs," which enabled App Developers to access content and information, including the content and information of users' Friends, beyond that available to non-whitelisted applications. According to Facebook's "Private Extended API Addendum," Whitelisted Apps could "retrieve data or functionality relating to Facebook ***that is not generally available under Platform***, which may include persistent authentication, photo upload, video upload, messaging and phonebook connectivity." (*Id.*)

102. Such whitelisting extended to thousands of companies. According to the DCMS Committee, Facebook's whitelisting "resulted in a large number of companies striking special deals," and "[a] November 2013 email discussion reveals that Facebook was managing 5,200 Whitelisted Apps, including Lyft, AirBnB, and Netflix."(*Id.*). Facebook granted these

whitelisted companies special access in exchange for value provided by those companies to Facebook. The level of access varied by agreement based on Facebook's relationship with the particular company and the purpose of the company's App. The Whitelisted Apps all entered into lucrative agreements with Facebook to purchase advertising. Those agreements conflict with Facebook's representations and statements to users regarding Graph API and its representations to users, in that Facebook stated Apps would no longer have access to users' Friends' data after May 2015. (See *Changelog—Graph API*, Facebook for Developers, https://web.archive.org/web/20141208030452/https://developers.facebook.com/docs/apps/changelog# (last visited on Feb. 20, 2019).

103. According to the DCMS Committee, "increasing revenues from major App developers was one of the key drivers behind the policy changes made by Facebook," and "[t]he idea of linking access to Friends' data to the financial value of the developers' relationship with Facebook was a recurring feature of the documents" considered by the DCMS Committee. (See DCMS Report at ¶ 87).

104. Facebook hid these whitelist agreements from users even after the 2018 Cambridge Analytica Scandal. In testimony to U.K. House of Commons, on April 26, 2018, Facebook's Chief Technical Officer Mike Schroepfer, responding to questions regarding the one-year transition period from Graph API v.1.0 to 2.0 during 2014 to 2015, failed to state that tens of companies were given special whitelist access beyond May 2015. (See Mike Schroepfer Testimony to U.K. House of Commons, *supra* note 147, at Q2202). This was a material omission by a key Facebook officer and executive.

105. A day later, Facebook provided a response to questions from German Congressional Committees regarding Cambridge Analytica. In its response, Facebook stated that in addition to public APIs, Facebook also has some APIs that are available only to certain partners for specific uses. Generally these APIs provide access to public information, such as to enable news and media organizations to follow breaking news. . . ." (See Facebook responses to open questions from the 'Committee on Legal Affairs and Consumer Protection' and the

'Committee on Digital Agenda', Facebook Newsroom (Apr. 27, 2018), https://fbnewsroomde.files.wordpress.com/2018/05/final-responses-to-german-committees.pdf)

106. That statement by Facebook in April 2018 failed to materially disclose or describe any of the whitelisted companies or what access they had to user's private information. Furthermore, contrary to this statement, Facebook granted tens of whitelisted companies access to users' non-public information.

107. Finally, the truth began to come to light on June 8, 2018, when the *Wall Street Journal* reported that Facebook struck whitelist deals allowing certain companies special access through APIs. (See Deepa Seetharaman and Kristen Grind, *Facebook Gave Some Companies Special Access to Additional Data About Users' Friends*, The Wall Street Journal (June 8, 2018), https://www.wsj.com/articles/facebook-gave-some-companies-access-to-additional-data-about-users- friends-1528490406). The report made clear that these agreements were separate from the custom deals Facebook entered into with Business Partners. The report also stated that Facebook struck these deals with "companies including Royal Bank of Canada and Nissan Motor Co., who advertised on Facebook or were valuable for other reasons." (*Id.*).

108. The fact show that Facebook granted special access to users' information based on the value a company brought to Facebook. In short, Facebook traded access to its users' information – without users' knowledge or consent – in exchange for whitelist companies' significant expenditures on Facebook advertising.

109. Facebook responded to this report, stating and admitting that a "small number" of partners had access to users' Friends after May 2015. But Facebook did not identify any further whitelisted companies, or state what information these Developers had access to.

110. Then, in response to questions posed by the U.S. House of Representative on

June 29, 2018, Facebook stated that 60 companies were "given a one-time extension of less than six months beyond May 2015 to come into compliance" with Facebook's new API. (See *Facebook's Response to House Energy and Commerce Questions for the Record*, at Pallone, Jr. § 4 ¶ 6; Letter from Facebook, Inc. to Chairman Greg Walden, Ranking Member Frank Pallone, Energy & Commerce Committee, and U.S. House of Representatives, *Facebook's Response to House Energy and Commerce Questions for the Record* at 22 (June 29, 2018), https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM- 20180411.pdf.). The list of companies includes:

- ABCSocial, ABC Television Network
- Actiance
- Adium
- Anschutz Entertainment Group
- AOL
- Arktan / Janrain
- Audi
- biNu
- Cerulean Studios
- Coffee Meets Bagel
- DataSift
- Dingtone
- Double Down Interactive
- Endomondo
- Flowics, Zauber Labs
- Garena
- Global Relay Communications
- Hearsay Systems
- Hinge
- HiQ International AB
- Hootsuite
- Krush Technologies
- LiveFyre / Adobe Systems
- Mail.ru
- MiggoChat
- Monterosa Productions Limited
- never.no AS
- NIKE

- Nimbuzz
- Nissan Motor Co. / Airbiquity Inc.
- Oracle
- Panasonic
- Playtika
- Postano, TigerLogic Corporation
- Raidcall
- RealNetworks, Inc.
- RegED / Stoneriver RegED
- Reliance / Saavn
- Rovi
- Salesforce / Radian6
- SeaChange International
- Serotek Corp.
- Shape Services
- Smarsh
- Snap
- Social SafeGuard
- Socialeyes LLC
- SocialNewsdesk
- Socialware / Proofpoint
- SoundayMusic
- Spotify
- Spredfast
- Sprinklr / Sprinklr Japan
- Storyful Limited / News Corp
- Tagboard
- Telescope
- Tradable Bits, TradableBits Media Inc.
- UPS
- Vidpresso
- Vizrt Group AS
- Wayin

111. According to Facebook, during this six-month extension, these companies continued to have access to the content and information of users and users' Friends. Facebook did not clarify why this group of companies were given special access to this content and information. Furthermore, subsequent reporting has revealed that some companies listed above were given

access beyond the six months, while additional companies should have been included on this list to Congress.

112. Next, on December 5, 2018, the UK Parliament released a cache of documents internal to Facebook. (See U.K. House of Commons, *Note by Damian Collins MP, Chair of the DCMS Committee: Summary of Key Issues from the Six4Three files* (Dec. 5, 2018), https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from- Six4Three.pdf)(*See also* UK Final Report HC1791, published 18 February 2019, by authority of the House of Commons). These documents consist of internal emails shared between Facebook employees; emails with outside Developers and Business Partners; and internal presentation materials. These documents showed a further series of undisclosed companies that Facebook traded whitelist access to. They include:

- Airbnb
- Badoo
- Bumble
- Hot or Not
- Lyft
- Netflix

113. The released documents reveal that Facebook granted these companies varying levels of access depending on the App's needs and on Facebook's relationship with the App. Several of the Apps listed above had access to non-App Friend lists. Others also had access to the private messages of App users. Facebook had its highest executive CEO Zuckerberg responded:

> We changed our platform policies in 2014/15 to prevent apps from requesting permission to access friends' information. The history of Cambridge Analytica shows this was the right thing to do. For most developers, we also limited their ability to request a list of who someone's friends were, unless those friends were also using the developer's app. **In some situations, when necessary, we allowed**

> **developers to access a list of the users' friends. This was not friends' private information but a list of your friends (name and profile pic).**
>
> . . .
>
> In addition, white lists are also common practice when testing new features and functionality with a limited set of partners before rolling out the feature more broadly (aka beta testing). Similarly, it's common to help partners transition their apps during platform changes to prevent their apps from crashing or causing disruptive experiences for users. (See Mark Zuckerberg, Facebook (Dec. 5, 2018), https://newsroom.fb.com/news/2018/12/response-to- six4three-documents/ (emphasis added).

114. Facebook's 12/5/2018 statement by CEO Zuckerberg is false because Facebook's internal emails and subsequent news articles have revealed that Hootsuite, Netflix, Royal Bank of Canada and Spotify also had access to more than just a name and profile pic, it allowed access to users' messenger mailbox, which would include messages sent from the users' Friends.

115. The 12/5/2018 CEO statement is also misleading. Since May 2010, users could set a non-public privacy designation for their Friends list at any time. Thus, even where the App User and her Friends set their Friends list to private, Whitelisted Apps who gained access to the App User's Friends list would still be able to see all of the Friends of that user. For Friends seeking to limit who could view their social connections, this was a violation of privacy.

116. On December 18, 2018, a *New York Times* investigation reported that Facebook had entered into over 150 previously undisclosed data sharing agreements with a variety of organizations. The report stated:

> "Facebook shared data with more than 150 companies — not only tech businesses but automakers and media organizations — through apps on its platform even if users disabled sharing. Apps from many of these "integration partners" never even showed up in user application settings, with the company considering them an extension of its own network. The deals dated back as far as 2010 and were all active in 2017, with some still in effect this year." (See *supra*, Dance, et al, New York Times).

117. The New York Times investigation article identified Spotify, Netflix and the Royal Bank of Canada as being able to "read, write and delete Facebook users' private message, and to see everyone on a message thread." (*Id.*). The report stated that Facebook's own internal documents show that these companies had access to users' messages beyond the time that the companies needed to integrate Facebook into their systems. For instance, "Spotify, which could view messages of more than 70 million users a month, still offers the option to share music through Facebook Messenger."(*Id.*). Yet, Facebook had previously misstated to Congress and identified Spotify in its list to Congress as only having access for six months beyond May 2015.

118. Facebook also had previously represented and purportedly removed access to users' mailboxes in Graph API v2.4, released on July 8, 2015, and had purportedly removed this permission for all APIs on October 6, 2015. (See *Changelog—Graph API*, Facebook for Developers,https://web.archive.org/web/20141208030452/https://developers.facebook.com/docs/apps/changelog# (last visited on Feb. 20, 2019). Thus, Facebook represented and users reasonably expected App Developers to no longer have access to any Facebook messages after October 2015 at the latest. However, as stated above, Facebook continued allowing many companies to access messages beyond that 2015 date.

C. Facebook Failed to Monitor and to Protect User Content and Information from Third Parties' Unauthorized Use.

119. While Facebook allowed third-party App Developers, whitelisted companies and Business Partners to access incredible amounts of users' content and information, Facebook failed to implement reasonable privacy and security measures, such as conducting regular audits and monitoring third parties' access and use of users' content and information. Facebook also failed to ensure that third parties complied with its Platform and Privacy policies. Facebook's

failure to act was a direct result of its reckless quest for profit growth at the expense of users' privacy.

F. Facebook Has a Pattern and History of Discarding Its Promises to Protect User Privacy in Reckless Pursuit of Growth.

120. Throughout its history, Facebook has repeatedly ignored users' privacy interests and its own representations to users to protect user content and information in a reckless and wanton quest to maximize its growth and maximize its profits. The Defendant has a history of privacy abuses and has used its highest executive officers to continually lie when making statements about its user privacy protections.

121. For example, starting back in 2006, Facebook launched its News Feed feature to display users' posts on their Friends' and networks' pages. This feature was immediately controversial because users' posts were automatically revealed regardless of users' intention to keep these posts private. Zuckerberg's response to this controversy was that "we did a bad job of explaining what the new features were and an even worse job of giving you control of them." (See Mark Zuckerberg, *An Open Letter From Mark Zuckerberg*, Facebook (Sept. 8, 2006), https://www.facebook.com/notes/facebook/an-open-letter-from-mark-zuckerberg/2208562130/.)

122. Then right after that, in 2007, Facebook launched Beacon, a feature that automatically shared users' website and App history with advertisers, who in turn shared users' activity with other Facebook users on the third-party sites. Users were not given the opportunity to opt-out of this feature, and were surprised to discover their formerly inaccessible activities had been repackaged and revealed by Facebook in order to attract Business Partners and advance its advertising program. Third-party participants in the Beacon program received user content and information, and the sites also gave Facebook ad-targeting data. After receiving privacy

complaints and a class action lawsuit, Beacon was shut down. In response, Zuckerberg stated, "We've made a lot of mistakes building this feature, but we've made even more with how we've handled them. We simply did a bad job with this release, and I apologize for it." (See Mark Zuckerberg, *Thoughts on Beacon*, Facebook (Dec. 5, 2007), https://www.facebook.com/notes/facebook/thoughts-on-beacon/7584397130/.). Yet, Facebook continued to violate users' expectation of privacy.

123. In May 2008, the Canadian Internet Policy and Public Interest Clinic ("CIPPIC") filed a complaint against Facebook with the Canadian Privacy Commissioner ("CPC") over a number of user privacy concerns, including the user content and information shared by Facebook with third party App Developers without express consent by users. The CPC launched an investigation in response to CIPPIC's complaint, which resulted in Facebook agreeing to user consent-centered reform in August 2009. The CPC's announcement indicated the following:

> Facebook has agreed to retrofit its application platform in a way that will prevent any application from accessing information until it obtains express consent for each category of personal information it wishes to access. Under this new permissions model, users adding an application will be advised that the application wants access to specific categories of information. The user will be able to control which categories of information an application is permitted to access. There will also be a link to a statement by the developer to explain how it will use the data. (See *News Release, Facebook Agrees to Address Privacy Commissioner's Concerns*, Office of the Privacy Commissioner of Canada (Aug. 27, 2009), https://www.priv.gc.ca/en/opc-news/news-and- announcements/2009/nr-c_090827/).

124. In November 2009, Facebook changed its Terms of Service to greatly expand the amount of personal information categorized as available to the public. *See supra*. In response to the change in privacy settings, ten privacy organizations, including the Electronic Privacy Information Center ("EPIC"), filed complaints to the FTC alleging that Facebook had changed users' privacy settings and disclosed personal content and information to third parties without

consent. EPIC warned "[t]he Facebook Platform transfers Facebook users' personal data to application developers without users' knowledge or consent.". (See *News Release, Facebook Agrees to Address Privacy Commissioner's Concerns*, Office of the Privacy Commissioner of Canada (Aug. 27, 2009), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2009/nr-c_090827/).

125. Defendant's CEO Zuckerberg responded with an apology to users, representing to the public and Facebook users that, "[s]ometimes we move too fast—and after listening to recent concerns, we're responding." (See Mark Zuckerberg, *From Facebook, Answering Privacy Concerns with New Settings*, The Wash. Post (May 24, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303828.html). Zuckerberg vowed to add privacy controls and further represented that privacy would be made stronger by representing that, "Many people choose to make some of their information visible to everyone so people they know can find them on Facebook. We already offer controls to limit the visibility of that information and we intend to make them even stronger. (*Id.*).

126. In October 2010, the *Wall Street Journal* reported that Facebook had been sending users' names and Facebook identification numbers to its advertisers without users' knowledge and consent. (See *Wall Street Journal* report, by Steel and Fowler, *supra)*.

127. Despite continuous and consistent feedback from users, privacy advocates, and regulators, in July 2010, while giving a speech at a technology awards show in San Francisco, CEO Zuckerberg announced that he believed privacy is no longer a "social norm.". (See Bobbie Johnson, *Privacy no longer a social norm, says Facebook founder*, The Guardian (Jan. 10, 2010), https://www.theguardian.com/technolog). CEO Zuckerberg stated, "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with

more people. That social norm is just something that has evolved over time." (*Id.*). Defendant CEO Zuckerberg's proclamation that social norms have changed, instead serves as an admission by Facebook to its pattern, practice and continued misrepresentations to attract users and a violations of users' privacy and trust.

128. On November 29, 2011, Facebook agreed to settle one of the rounds of FTC charges, which alleged that Facebook had deceived users by telling them they could keep their information on Facebook private and then repeatedly allowed it to be shared and made public without the user's consent. The FTC adopted the final Consent Order on August 10, 2012. The order requires Facebook to take steps including, "giving consumers clear and prominent notice and obtaining their express consent before sharing their information beyond their privacy settings, by maintaining a comprehensive privacy program to protect consumers' information, and by obtaining biennial privacy audits from an independent third party.". (See *FTC approves Final Settlement With Facebook*, Federal Trade Commission (Aug. 10, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook.)

129. In May 2018, at Facebook's f8 conference, Zuckerberg announced plans to add a "Clear History" feature that would enable users to see the websites and Apps that send their information to Facebook when they use them. Zuckerberg promised that this feature would allow users to "clear this information from their accounts, and turn off [Facebook's] ability to store it . . . going forward." CEO Zuckerberg made this announcement in the wake of the Cambridge Analytica Scandal and claimed Facebook would release this feature "in the coming months," but was delayed and released in early 2020 far after the class action lawsuit for these privacy torts was filed. (See Chris Welch, *Facebook to introduce clear history privacy tool in coming months*, Verge (May 1, 2018), https://www.theverge.com/2018/5/1/17307346/facebook-clear-history-

new-privacy-feature.).

130. In 2016, Andrew Bosworth, a vice president at Facebook, admitted to the company's growth tactics in an internal memo. Bosworth's memo explains that despite any ramifications, Facebook's growth is what he called "*de facto* good" as quoted below:

> The ugly truth is that we believe in connecting people so deeply that anything that allows us to connect more people more often is *de facto* good. It's perhaps the only area where the metrics do tell the true story as far as we are concerned.
> . . .
> [M]ake no mistake, growth tactics are how we got here. If you joined the company because it is doing great work, that's why we get to do that great work. We do have great products but we still wouldn't be half our size without pushing the envelope on growth. Nothing makes Facebook as valuable as having your friend on it, and no product decisions have gotten as many friends on as the ones made in growth.[204]

131. At least by the end of 2015, Facebook had actual knowledge that Plaintiffs' content and information had been accessed, downloaded by third parties, and misused without users' authorization. Further, Facebook was aware that such misuse of Plaintiffs' data presented substantial risk of further misuse, fraud, and identity theft to Plaintiffs. Despite this knowledge, and in contravention of its repeated assurances to users that privacy and trust were important parts of Facebook's service, Facebook failed to provide notification to Plaintiffs of the misuse of their content and information without and/or in excess of users' authorization, until March 2018—more than two years after it was informed of the Cambridge Analytica Scandal.

In the years from 2015 and 2018, Facebook failed to inform Plaintiffs that their sensitive content and information had been used without and/or in excess of their authorization. As a result of this failure, Facebook failed to allow users the opportunity to take steps to protect themselves and mitigate their heightened risk of identity theft and other harms.

132. Plaintiffs did not learn of Facebook's suppression of facts until after the media reported that Facebook had permitted unauthorized third parties to access and retain user content and information without and/or in excess of users' authorization, and that their content and information was allegedly used by Cambridge Analytica to create targeted psychographic messaging and advertising on behalf of President Donald J. Trump's Presidential campaign.

133. It is undisputed that the Nationwide Class Action included an express sub-class for Georgia residents and Georgia laws. The filing of the Nationwide Class Action Complaint, Settlement and Opt-Out has tolled the Plaintiffs' statute of limitations since that time.

FTC ACTION

134. On November 29, 2011, Facebook agreed to settle one of the rounds of FTC charges, which alleged that Facebook had deceived users by telling them they could keep their information on Facebook private and then repeatedly allowed it to be shared and made public without the user's consent. The FTC adopted the final Consent Order on August 10, 2012. The Order requires Facebook to take steps including, "giving consumers clear and prominent notice and obtaining their express consent before sharing their information beyond their privacy settings, by maintaining a comprehensive privacy program to protect consumers' information, and by obtaining biennial privacy audits from an independent third party.". (See *FTC approves Final Settlement With Facebook*, Federal Trade Commission (Aug. 10, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook.)

135. In May 2014, after years of controversy, Facebook represented to users that it restored the default Privacy Setting of"Friends Only" for Posts for new users, but did not change settings for existing users. (Josh Constine, *Facebook Stops Irresponsibly Defaulting Privacy of New Users' Posts to "Public," Changes to*

"Friends," TechCrunch (May 22, 2014), https://techcrunch.com/2014/05/22/sometimes- less-open-is-more.). Rather, Facebook offered existing users "Privacy Check-ups" that continued to recommend public disclosure of nearly all user content and information. Facebook also made the setting for posts "sticky," meaning that new posts defaulted to whatever setting was selected for the previous post. These user-content default settings have largely remained in place since 2014, though Facebook has made adjustments to the location and availability of privacy settings and controls. (Daniel Terdiman, *Facebook Just Announced These Changes To Try To Ease Your Mind On Privacy And Data*, Fast Company (Mar. 28, 2018) https://www.fastcompany.com/40550689/how-facebook-is-striving-to-ease-users-minds-on-privacy-and-data). Notably absent from Facebook's "Sharing Recommendations" seen below, is that the privacy settings fail to contain any selection for choices of sharing with any of Facebook's third-parties or Business Partners.

136. On July 24, 2019, the FTC issued a press release stating that, again, Facebook had violated user privacy *and also* the prior 2012 FTC Consent Order. The FTC Chairman stated "that Facebook failed to live up to its commitments under that order. Facebook subsequently made similar misrepresentations about sharing consumer data with third-party apps and giving users control over that sharing, and misrepresented steps certain consumers needed to take to control facial recognition technology." (See July 24, 2019 FTC Statement of Chairman Joe Simons). Facebook agreed to a Stipulated Order and paid a government fine of $5 billion. The fine is less than .6 % (.006) of the company value of Meta.

CAUSES OF ACTION

Count One: Fraud in the Inducement

137. Plaintiff adopts and realleges each and every allegation set forth in the paragraphs above as if they were fully set forth herein.

138. On November 29, 2011, Facebook agreed to settle one of the rounds of FTC charges, which alleged that Facebook had deceived users by telling them they could keep their information on Facebook private and then repeatedly allowed it to be shared and made public without the user's consent. The FTC adopted the final Consent Order on August 10, 2012. The Order requires Facebook to take steps including, "giving consumers clear and prominent notice and obtaining their express consent before sharing their information beyond their privacy settings, by maintaining a comprehensive privacy program to protect consumers' information, and by obtaining biennial privacy audits from an independent third party.". (See *FTC approves Final Settlement With Facebook*, Federal Trade Commission (Aug. 10, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook.)

139. In May 2014, after years of controversy, Facebook represented to users that it restored the default Privacy Setting of "Friends Only" for Posts for new users, but did not change settings for existing users. (Josh Constine, *Facebook Stops Irresponsibly Defaulting Privacy of New Users' Posts to "Public," Changes to "Friends,"* TechCrunch (May 22, 2014), https://techcrunch.com/2014/05/22/sometimes- less-open-is-more.). Rather, Facebook offered existing users "Privacy Check-ups" that continued to recommend public disclosure of nearly all user content and information. Facebook also made the setting for posts "sticky," meaning that new posts defaulted to whatever setting was selected for the previous post. These user-content default settings have largely remained in place since 2014, though Facebook has made adjustments to the location and

availability of privacy settings and controls. (Daniel Terdiman, *Facebook Just Announced These Changes To Try To Ease Your Mind On Privacy And Data*, Fast Company (Mar. 28, 2018) https://www.fastcompany.com/40550689/how-facebook-is-striving-to-ease-users-minds-on-privacy-and-data). Notably absent from Facebook's "Sharing Recommendations" seen below, is that the privacy settings fail to contain any selection for choices of sharing with any of Facebook's third-parties or Business Partners.

140. On July 24, 2019, the FTC issued a press release stating that, again, Facebook had violated user privacy *and also* the prior 2012 FTC Consent Order. The FTC Chairman stated "that Facebook failed to live up to its commitments under that order. Facebook subsequently made similar misrepresentations about sharing consumer data with third-party apps and giving users control over that sharing, and misrepresented steps certain consumers needed to take to control facial recognition technology." (See July 24, 2019 FTC Statement of Chairman Joe Simons). Facebook agreed to a Stipulated Order and paid a government fine of $5 billion. The fine is less than .6 % (.006) of the company value of Meta.

141. Defendant undertook a duty to represent to the Plaintiffs its control and use of Plaintiffs' private information and property to induce the Plaintiffs to "upload" or otherwise generate personal information from their personal cell phones and mobile internet device. Defendants achieved its fraudulent conduct by representing that Plaintiffs could protect their information through the "privacy" settings in the Facebook "settings" located on the Plaintiff's cell phones and/or internet device.

142. Plaintiffs' personal data, photos, property and private information was created and/or maintained on their personal cell phones or internet device located in this County. Plaintiffs' selection of the "settings" in Facebook occurred in this County through the use of Plaintiffs'

internet device.

143. Defendant misrepresented the use of Plaintiffs' property, data, private information and the way that it recorded, maintained, sold and stored Plaintiff's personal information.

144. Plaintiffs relied on the representations made by Meta and its predecessor, to their detriment, and engaged Defendant's Facebook user experience.

145. Plaintiffs did not discover and could not have reasonably discovered the internal Facebook fraud and suppressions of fact by Facebook until after the April 4, 2018 Facebook press release, or the June 8, 2018 *Wall Street Journal* report, and actually discovered that they were deceived upon learning of the notice of their inclusion and opt out of the class action settlement after June 2023.

146. As a direct and proximate result of the fraudulent inducement conduct of Defendant, each named Plaintiff was injured and damaged by loss of their private information, data, loss of their privacy, suffered mental anguish and emotional distress.

WHEREFORE, PREMISES CONSIDERED, each Plaintiff respectfully requests this Honorable Court to enter judgment against Defendant, award compensatory damages and punitive damages in an amount determined by a jury, court costs and interest as allowed by law, and any all other relief as the Court deems just and proper.

Count Two: Invasion of Privacy

147. Each Plaintiff adopts and realleges each and every allegation set forth in the paragraphs above as if they were fully set forth herein.

148. Defendant intruded into each Plaintiff's private activities in such a manner to outrage

or cause mental suffering, shame, or humiliation in numerous ways, including intruding into the plaintiff's physical solitude or seclusion, using private information about the plaintiff that violates ordinary decency, putting the plaintiff in a false but not necessarily defamatory position to Defendant's business partners, and/or by appropriating some element of the Plaintiff's personality for a commercial use.

149. The conduct Defendant was intentional, fraudulent, wanton, reckless, and/or oppressive.

150. As a direct and proximate result of the invasion of each Plaintiff's privacy by Defendant, Plaintiff was injured and damaged by loss of their private information, data, loss of their privacy, suffered mental anguish and emotional distress.

151. Defendant is vicariously liable for the conduct of their employees and those they reserved a right to control under the doctrine of respondeat superior.

WHEREFORE, PREMISES CONSIDERED, each named Plaintiff respectfully requests this Honorable Court to enter judgment against Defendant, award compensatory damages in an amount determined by a jury, punitive damages in an amount determined by a jury to punish the Defendant for its wrongful conduct and the wrongful conduct of their employees and those they reserved a right to control. Punitive damages are due to be awarded in an amount to deter this Defendant and others from committing the same or similar wrongful conduct in the future, court costs and interest as allowed by law, and any all other relief as the Court deems just and proper.

Count Three: Conversion

152. Each Plaintiff adopts and realleges each and every allegation set forth in the paragraphs above as if they were fully set forth herein.

153. Defendant undertook a wrongful exercise of dominion over each Plaintiff's property

in defiance of each Plaintiff's rights, and violated each Plaintiff's immediate rights of possession to the property, data and information. Defendant Meta's actions are a wrongful detention or interference with each Plaintiff's property.

154. Defendant has converted each Plaintiff's property for Defendant's own use and benefit. Upon information and belief, Defendant is a publicly traded company on the NASDAQ stock market and has created revenue and company value by, *inter alia*, the conversion of user's personal property, data and information, including Plaintiffs and more than another 2.8 million Georgia citizens.

155. As a direct and proximate result of the conversion and civil theft of each Plaintiff's property and data by Defendant, Plaintiff was injured and damaged by loss of their private property, information, data, loss of their privacy, suffered mental anguish and emotional distress.

156. Defendant is vicariously liable for the conduct of their employees and those they reserved a right to control under the doctrine of respondeat superior.

WHEREFORE, PREMISES CONSIDERED, each named Plaintiff respectfully requests this Honorable Court to enter judgment against Defendant for conversion of property, award compensatory damages in an amount determined by a jury, punitive damages in an amount determined by a jury to punish the Defendant for its wrongful conduct and the wrongful conduct of their employees and those they reserved a right to control. Punitive damages are due to be awarded in an amount to deter this Defendant and others from committing the same or similar wrongful conduct in the future, court costs and interest as allowed by law, and any all other relief as the Court deems just and proper.

Count Four: Intentional Infliction of Emotional Distress

157. Plaintiff adopts and realleges each and every allegation set forth in the paragraphs above as if they were fully set forth herein.

158. The conduct of Defendant was intentional or reckless, was extreme and outrageous, was beyond all possible bounds of decency, was atrocious and utterly intolerable in a civilized society, and caused emotional distress so severe that no reasonable person could be expected to endure it.

159. The conduct Defendant was intentional, fraudulent, wanton, reckless, and/or oppressive.

160. As a direct and proximate result of the outrageous conduct of Defendant, each named Plaintiff was injured and damaged by loss of their private information, data, loss of their privacy, suffered mental anguish and emotional distress.

161. Defendant is vicariously liable for the conduct of their employees and those they reserved a right to control under the doctrine of respondeat superior.

WHEREFORE, PREMISES CONSIDERED, each Plaintiff respectfully requests this Honorable Court to enter judgment against the Defendant, award compensatory damages in an amount determined by a jury, punitive damages in an amount determined by a jury to punish this Defendant for their wrongful conduct and the wrongful conduct of their employees and those they reserved a right to control and to deter this Defendant and others from committing the same or similar wrongful conduct in the future, court costs and interest as allowed by law, and any all other relief as the Court deems just and proper.

Count Five: Willfulness and Wantonness Claims

162. Plaintiff adopts and realleges each and every allegation set forth in the paragraphs above

as if they were fully set forth herein.

163. Defendants, their employees, and those they reserved a right to control acted willfully with the intent of harming Plaintiff.

164. In the alternative, they acted consciously, knowing that harm would likely or probably result to Plaintiff and/or similarly situated individuals, but without the specific knowledge that harm would absolutely result.

165. Defendants as institutions acted consciously, knowing that harm would likely or probably result to Plaintiff and/or similarly situated individuals, but without the specific knowledge that harm would absolutely result.

166. The conduct Defendants, their employees, and those they reserved a right to control was intentional, fraudulent, wanton, reckless, and/or oppressive.

167. As a direct and proximate result of the willful and/or wanton conduct of the Defendant, Plaintiff was injured and damaged by loss of their private information, data, loss of their privacy, suffered mental anguish and emotional distress.

168. Defendant is vicariously liable for the conduct of their employees and those they reserved a right to control under the doctrine of respondeat superior.

WHEREFORE, PREMISES CONSIDERED, each Plaintiff respectfully requests this Honorable Court to enter judgment against Defendant, award compensatory damages in an amount determined by a jury, punitive damages in an amount determined by a jury to punish this Defendant for its wrongful conduct and the wrongful conduct of their employees and those they reserved a right to control and to deter this Defendant and others from committing the same or similar wrongful conduct in the future, court costs and interest as allowed by law, and any all other relief as the Court deems just and proper.

****Plaintiff Demands a Trial by Jury****

Respectfully submitted this 31st day of October, 2023,

/s/ William Gregory Dobson
WILLIAM GREGORY DOBSON
Georgia State Bar No. 237770
MICHAEL J. LOBER
Georgia State Bar No. 455580
TODD L. LORD
Georgia State Bar No. 457855
Attorneys for Plaintiffs

Lober & Dobson, LLC
830 Mulberry St.
Suite 201-Robert E. Lee Building
Macon, Georgia 31201
(478) 745-7700
wgd@lddlawyers.com
mjlober@lddlawyers.com

Law Office of Todd L. Lord
4 Courthouse Square
P.O. Box 901
Cleveland, Georgia 30528
(706) 219-2239
attytllord@windstream.net